

#3

Docket No. 1614.1010/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Tsuneo SATO et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: November 16, 1999

For: **DEVICE AND METHOD FOR USER IDENTIFICATION CHECK BASED
ON USER-SPECIFIC FORMULA**



**SUBMISSION OF CERTIFIED COPY OF PRIOR
FOREIGN APPLICATION IN ACCORDANCE WITH
THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application(s):


Japanese Patent Application No. 11-113058
Filed: April 21, 1999

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date, as evidenced by the certified papers attached hereto, in accordance with the requirements
of 35 U.S.C. § 119.

Respectfully submitted,
STAAS & HALSEY LLP

Date: November 16, 1999

By: _____


H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC675 U.S. PTO
09/441081
11/16/99

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1 9 9 9 年 4 月 2 1 日

出 願 番 号
Application Number:

平成 1 1 年 特 許 願 第 1 1 3 0 5 8 号

出 願 人
Applicant (s):

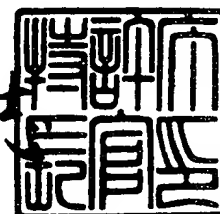
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1 9 9 9 年 8 月 3 0 日

特 許 庁 長 官
Commissioner,
Patent Office

山 建 佐 平



出証番号 出証特平 1 1 - 3 0 6 0 1 0 4

【書類名】 特許願

【整理番号】 9900952

【提出日】 平成11年 4月21日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/00

【発明の名称】 ユーザ認証装置及び方法とユーザ認証用カードとプログラム記録媒体

【請求項の数】 11

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 佐藤 恒夫

【発明者】

 【住所又は居所】 大分県大分市東春日町17番58号 株式会社富士通大分ソフトウェアラボラトリ内

 【氏名】 古手川 清

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100095072

 【弁理士】

 【氏名又は名称】 岡田 光由

 【電話番号】 03-3807-1818

【選任した代理人】

 【識別番号】 100074848

 【弁理士】

 【氏名又は名称】 森田 寛

【手数料の表示】

【予納台帳番号】 012944

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707817

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ユーザ認証装置及び方法とユーザ認証用カードとプログラム記録媒体

【特許請求の範囲】

【請求項 1】 ユーザ認証に用いるユーザ認証装置であって、

ユーザに提示される乱数とユーザ認証対象に対応した計算式とから、ユーザ認証に用いる数値を算出する算出手段と、

上記乱数の提示に応答して入力されてくる数値と、上記算出手段の算出する数値とが一致するの否かを判断する判断手段とを備えることを、

特徴とするユーザ認証装置。

【請求項 2】 請求項 1 記載のユーザ認証装置において、

算出手段は、計算式が演算子を含まない数字列である場合には、その数字列を算出結果とすることを、

特徴とするユーザ認証装置。

【請求項 3】 請求項 1 又は 2 記載のユーザ認証装置において、

算出手段は、計算式がユーザ認証時に応じて変化する変数値を含む場合には、ユーザに提示する乱数とユーザ認証対象に対応した計算式と該変数値とから、ユーザ認証に用いる数値を算出することを、

特徴とするユーザ認証装置。

【請求項 4】 ユーザ認証に用いるユーザ認証装置であって、

ユーザ ID とユーザ認証対象に対応した計算式との対応関係を管理する管理手段と、

上記管理手段の管理データから、指定されるユーザ ID に対応付けられる計算式を特定する特定手段と、

ユーザに提示される乱数と上記特定手段の特定する計算式とから、ユーザ認証に用いる数値を算出する算出手段と、

上記乱数の提示に応答して入力されてくる数値と、上記算出手段の算出する数値とが一致するの否かを判断する判断手段とを備えることを、

特徴とするユーザ認証装置。

【請求項 5】 請求項 4 記載のユーザ認証装置において、
ユーザから入力されてくる計算式と、管理手段に管理される該ユーザ ID の指
す計算式とが一致することを条件にして、管理手段に管理される計算式を更新す
る更新手段を備えることを、

特徴とするユーザ認証装置。

【請求項 6】 請求項 4 又は 5 記載のユーザ認証装置において、
算出手段は、管理手段に管理される計算式が演算子を含まない数字列である場
合には、その数字列を算出結果とすることを、

特徴とするユーザ認証装置。

【請求項 7】 請求項 4、5 又は 6 記載のユーザ認証装置において、
算出手段は、管理手段に管理される計算式がユーザ認証時に応じて変化する変
数値を含む場合には、ユーザに提示する乱数とユーザ認証対象に対応した計算式
と該変数値とから、ユーザ認証に用いる数値を算出することを、

特徴とするユーザ認証装置。

【請求項 8】 ユーザ認証に用いるユーザ認証方法であって、
ユーザに提示される乱数とユーザ認証対象に対応した計算式とから、ユーザ認
証に用いる数値を算出する第 1 の処理過程と、

上記乱数の提示に回答して入力されてくる数値と、第 1 の処理過程で算出した
数値とが一致するの可否かを判断する第 2 の処理過程とを備えることを、

特徴とするユーザ認証方法。

【請求項 9】 カードの所有者の認証用に用意されるユーザ認証用カードに
おいて、

ユーザ ID を記録することに加えて、ユーザ認証対象に対応した計算式を記録
するように構成されることを、

特徴とするユーザ認証用カード。

【請求項 10】 請求項 9 記載のユーザ認証用カードにおいて、
ユーザ認証対象に対応した計算式に代入される乱数を発生する乱数発生手段を
備えることを、

特徴とするユーザ認証用カード。

【請求項 11】 ユーザ認証に用いるユーザ認証装置の実現に用いられるプログラムが格納されるプログラム記録媒体であって、

ユーザに提示される乱数とユーザ認証対象に対応した計算式とから、ユーザ認証に用いる数値を算出する算出処理と、

上記乱数の提示に応答して入力されてくる数値と、上記算出処理の算出する数値とが一致するの可否かを判断する判断処理とをコンピュータに実行させるプログラムが格納されることを、

特徴とするプログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ユーザ認証に用いるユーザ認証装置及び方法と、カードの所有者の認証用に用意されるユーザ認証用カードと、ユーザ認証装置の実現に用いられるプログラムが格納されるプログラム記録媒体とに関し、特に、ユーザやシステムに負荷をかけることなく高いセキュリティを実現するユーザ認証装置及び方法と、ユーザやシステムに負荷をかけることなく高いセキュリティを実現するユーザ認証用カードと、そのユーザ認証装置の実現に用いられるプログラムが格納されるプログラム記録媒体とに関する。

【0002】

コンピュータ社会の発達により、様々な情報処理分野で、コンピュータを使ったユーザ認証が行われるようになってきた。このユーザ認証が誤ったり悪用されたりすると、個人に多大な損害を及ぼすとともに、社会に大きな混乱を招くことになる。これから、高いセキュリティを実現するユーザ認証技術の構築が叫ばれている。

【0003】

【従来の技術】

最も広く用いられているユーザ認証技術としては、ユーザに4桁などで定義される暗証番号を登録させる構成を採って、ユーザ認証の必要があるときに、ユーザに自分の暗証番号を入力させ、その入力させた暗証番号と登録されている暗証

番号とが一致するの否かをチェックしていくことで、正規のユーザであるの否かをチェックしていくという方法がある。

【0004】

しかしながら、従来技術のように、絶対的な数値で定義される絶対的な暗証番号を用いる場合、ユーザが暗証番号を入力しているときに、その暗証番号を他人に見られてしまうと、その暗証番号の秘密性がなくなることで、高いセキュリティを実現できないという問題点がある。

【0005】

更に、従来技術のように、絶対的な数値で定義される絶対的な暗証番号を用いる場合、ユーザは、暗証番号として、電話番号や生年月日や住所番号など自分に関係する覚えやすい数値を用いることが多く、これから、この従来技術に従っていると、他人に暗証番号が知られる可能性が高いことで、高いセキュリティを実現できないという問題点もある。

【0006】

このような問題点の解決を図るために、特開昭63-170764号で、ユーザに対して、計算式と固有値とを登録させる構成を採るとともに、ユーザ認証時に時間に依存して変化する変数を発生させる構成を採って、ユーザ認証の必要があるときに、発生変数をその計算式に代入した結果がその固有値となる数値をユーザに入力させ、その入力させた数値とシステムの計算結果とが一致するの否かをチェックしていくことで、正規のユーザであるの否かをチェックするという技術が開示された。

【0007】

この特開昭63-170764号で開示されたユーザ認証技術では、例えば、ユーザは、予め計算式「 $x + y$ 」と固有値「 $z_0 = 7$ 」とを登録しておき、時間に依存して変化する変数 x の値として「3」が表示されるときには、「 $x + y = 7$ 」を実現する「 $y = 4$ 」を入力していくことで、本人であることを入力できるようになる。

【0008】

【発明が解決しようとする課題】

確かに、特開昭63-170764 号で開示されたユーザ認証技術に従うと、ユーザは、暗証番号のような固定の数値を入力する訳ではないので、入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるというメリットが得られる。

【0 0 0 9】

しかしながら、この特開昭63-170764 号で開示されたユーザ認証技術に従うと、ユーザは、自分の登録した計算式と固有値との両方を覚えていなければならないとともに、固有値から逆算していくという暗算を行わなければならない、大きな負荷を強いられるという問題点がある。

【0 0 1 0】

更に、システムは、ユーザの登録した計算式と固有値との両方をメモリに記憶しなければならない、大きなメモリ容量を強いられるという問題点がある。

【0 0 1 1】

本発明はかかる事情に鑑みてなされたものであって、ユーザやシステムに負荷をかけることなく高いセキュリティを実現する新たなユーザ認証装置及び方法の提供と、ユーザやシステムに負荷をかけることなく高いセキュリティを実現する新たなユーザ認証用カードの提供と、そのユーザ認証装置の実現に用いられるプログラムが格納される新たなプログラム記録媒体の提供とを目的とする。

【0 0 1 2】

【課題を解決するための手段】

図1に本発明の原理構成を図示する。

【0 0 1 3】

図中、1は本発明を具備するユーザ認証装置であって、ユーザ認証処理を実行するもの、2はユーザ認証装置1の備える端末であって、ユーザとの対話手段となるものである。

【0 0 1 4】

本発明のユーザ認証装置1は、管理手段10と、登録更新手段11と、乱数発生手段12と、特定手段13と、算出手段14と、判断手段15とを備える。

【0 0 1 5】

この管理手段10は、ユーザIDとユーザ認証対象に対応した計算式（単なる数字列のこともある）との対応関係を管理する。登録更新手段11は、ユーザと対話することで、管理手段10に計算式を登録したり、管理手段10に登録される計算式を更新する。乱数発生手段12は、規定の数の数字列からなる乱数（1つの数字のこともある）を発生してユーザに提示する。

【0016】

特定手段13は、管理手段10の管理データから、指定されるユーザIDに対応付けられる計算式を特定する。算出手段14は、乱数発生手段12の発生する乱数と特定手段13の特定する計算式とから、ユーザ認証に用いる数値を算出する。判断手段15は、乱数発生手段12の提示する乱数に応答して入力されてくる数値と、算出手段14の算出する数値とが一致するの可否かを判断することでユーザ認証を実行する。

【0017】

ここで、本発明のユーザ認証装置1の持つ機能は具体的にはプログラムで実現されるものであり、このプログラムは、フロッピーディスクなどに格納されたり、サーバなどのディスクなどに格納され、それらからユーザ認証装置1にインストールされてメモリ上で動作することで、本発明を実現することになる。

【0018】

このように構成される本発明のユーザ認証装置1では、登録更新手段11は、端末2から入力されてくる計算式（単なる数字列のこともある）を受け取り、ユーザIDとの対応を取りつつ、その計算式を管理手段10に登録することで、管理手段10に対して、ユーザIDとユーザ認証対象に対応した計算式との対応関係を登録する。そして、管理手段10に登録した計算式の更新要求があるときには、端末2から、その計算式と一致する計算式が入力されてくることを条件にして、その計算式に代わる新たな計算式を受け取り、それによって管理手段10に登録した計算式を更新する。

【0019】

このようにして、登録更新手段11の処理に従って、管理手段10に、ユーザIDとユーザ認証対象に対応した計算式（単なる数字列のこともある）との対応

関係が管理されることになる。

【0020】

この管理手段10の管理データを受けて、ユーザIDを指定してユーザ認証の要求が発行されると、特定手段13は、管理手段10の管理データから、そのユーザIDに対応付けられる計算式を特定する。一方、乱数発生手段12は、乱数を発生して、端末2のディスプレイ画面に表示するとともに、その発生した乱数を算出手段14に通知する。

【0021】

これを受けて、算出手段14は、乱数発生手段12の発生した乱数と特定手段13の特定した計算式とから、ユーザ認証に用いる数値を算出する。そして、判断手段15は、乱数発生手段12の提示した乱数に応答して端末2からの入力されてくる数値と、算出手段14の算出した数値とが一致するの可否かを判断することでユーザ認証を実行する。

【0022】

このときに、算出手段14は、計算式として演算子を含まない数字列が特定される場合には、その数字列を算出結果としていくことで、従来から用いられている数字列の暗証番号の利用を可能にする。

【0023】

また、算出手段14は、計算式がユーザ認証時に応じて変化する変数値（例えば、ユーザ認証時が1月～12月のときに、それらの月のそれぞれに数字“1”～“12”を割り付けるような場合）を含む場合には、乱数発生手段12の発生した乱数と特定手段13の特定した計算式とその変数値とから、ユーザ認証に用いる数値を算出することになる。

【0024】

ここで、ユーザ認証時に応じて変化する変数値としては、ユーザ認証時の年月日（yy yy. mm. dd）、時刻（hh. mm. ss）、AM/PM（“AM”=0、“PM”=1など）、曜日（“月曜日”=1、“火曜日”=2、・・・など）の一部又は全てを組み合わせ用いることができる。

【0025】

このようにして、本発明のユーザ認証装置 1 では、ユーザ認証対象に対応した計算式を登録し、乱数を発生してユーザに提示する構成を採って、暗証番号の代わりに、その乱数の提示に応答してユーザから入力される数値と、その計算式とその乱数とから算出される数値との一致をチェックしていくことでユーザ認証を実行する構成を採ることから、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。

【0026】

そして、ネットワーク環境で使用される場合に、ユーザ認証対象に対応した計算式を転送しない構成を採ること、暗証番号を転送する従来技術に比べて、高いセキュリティを実現できるようになる。

【0027】

しかも、特開昭63-170764 号で開示されたユーザ認証技術に従うと、ユーザは計算式と固有値との両方を覚えなくてはならないのに対して、本発明では、ユーザは計算式のみを覚えれば足りるとともに、特開昭63-170764 号で開示されたユーザ認証技術に従うと、システムは計算式と固有値との両方をメモリに記憶しなければならないのに対して、本発明では、システムは計算式のみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

【0028】

そして、本発明のユーザ認証装置 1 に合わせて、カードの所有者の認証用に用意される本発明のユーザ認証用カードでは、暗証番号に代えて、ユーザ認証対象に対応した計算式を記録する構成を採り、これにより、従来技術よりも高いセキュリティを実現できるようになる。

【0029】

【発明の実施の形態】

以下、実施の形態に従って本発明を詳細に説明する。

【0030】

図 2 に、本発明を具備する情報処理装置 20 の一実施例を図示する。

【0031】

この実施例に従う本発明を具備する情報処理装置 20 は、CRT などのディスプレイ装置 21 と、マウスなどの入力装置 22 と、ユーザ認証処理に必要となるデータを格納する認証用管理ファイル 23 と、フロッピーディスクや回線などを介してインストールされて、認証用管理ファイル 23 の管理データの登録更新処理を実行する認証用管理プログラム 24 と、フロッピーディスクや回線などを介してインストールされて、認証用管理ファイル 23 の管理データを使ってユーザ認証処理を実行する認証プログラム 25 とを備える。

【0032】

図 3 に、認証用管理ファイル 23 の管理データの一実施例を図示する。

【0033】

この図に示すように、認証用管理ファイル 23 は、ユーザの ID と、そのユーザの登録したパスワードロジック（暗証番号のこともある）との対応関係を管理する。

【0034】

このパスワードロジックは、認証プログラム 25 の発生する乱数に対する計算式を定義するものであって、この図の例では、例えば、ユーザ ID “000005” のユーザは、“ABCD” という数字列で表される乱数に対して、数字 A と数字 B との差分値を算出するというパスワードロジックを定義して、それを認証用管理ファイル 23 に登録し、また、ユーザ ID “000004” のユーザは、パスワードロジックの代わりに従前通りの “5384” という数字列で表される暗証番号を定義して、それを認証用管理ファイル 23 に登録している。

【0035】

図 3 の実施例では、説明の便宜上、認証用管理ファイル 23 に格納されるパスワードロジックを一般的な算術式で記載したが、この計算式は、実際には、例えば逆ポーランド法のような記述形式で記憶されることになる。

【0036】

逆ポーランド法の記述形式に従うと、図中に示す「 $10 \times A$ 」は「 $10A*$ 」、「 $A \times A$ 」は「 $AA*$ 」、「 $A \div B$ 」は「 $AB/$ 」、「 $A - B$ 」は「 $AB-$ 」、「 $(B - A) + C$ 」は「 $BA-C+$ 」、「 $((A - B) \times 5) \div 2$ 」は「 $AB-$

5 * 2 /」と表される。このような記述形式に従う方が分かり難いので、セキュリティを高めることができる。

【0037】

図4及び図5に、認証用管理プログラム24の実行する処理フローの一実施例、図6及び図7に、認証プログラム25の実行する処理フローの一実施例を図示する。次に、これらの処理フローに従って、図2のように構成される実施例の処理について説明する。

【0038】

認証用管理プログラム24は、ユーザからパスワードロジックの登録要求が発行されると、図4の処理フローに示すように、先ず最初に、ステップ1で、ディスプレイ装置21に、図8に示すようなパスワードロジック登録画面を表示する。

【0039】

続いて、ステップ2で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザIDを入力し、続くステップ3で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザの定義するパスワードロジックを入力する。

【0040】

後述するように、認証プログラム25は数字列“ABCD”（各数字は0か自然数）で表される4桁の乱数を発生するので、ユーザは、自分のパスワードロジックとして、これらの数字A／数字B／数字C／数字Dに対する四則演算（全ての数字を使う必要はない。括弧を使うことも許される）を定義することができ、認証用管理プログラム24は、このユーザの定義するパスワードロジックを入力することになる。ここで、ユーザは、従前通りの暗証番号を使用することを希望するときには、4桁で定義される暗証番号を入力するので、このときには、認証用管理プログラム24は、このユーザの定義する暗証番号を入力することになる。

【0041】

続いて、ステップ4で、ユーザがパスワードロジック登録画面の終了ボタン（

登録実行を指示するボタン)を操作したのか否かを判断して、終了ボタンではなくてキャンセルボタンを操作したことを判断するときには、そのまま処理を終了し、終了ボタンを操作したことを判断するときには、ステップ5に進んで、そのユーザのパスワードロジックが既に認証用管理ファイル23に登録されているのか否かを判断する。

【0042】

このステップ5の判断処理に従って、そのユーザのパスワードロジックが既に認証用管理ファイル23に登録されていることを判断するときには、ステップ6に進んで、ステップ3で入力したパスワードロジックの登録不可を表示すべく、ディスプレイ装置21に、既にパスワードロジックが登録されている旨を出力して処理を終了する。

【0043】

一方、ステップ5で、そのユーザのパスワードロジックが未だ認証用管理ファイル23に登録されていないことを判断するときには、ステップ7に進んで、ステップ3で入力したパスワードロジックをそのユーザのIDと対応をとりつつ、認証用管理ファイル23に登録して処理を終了する。

【0044】

このようにして、認証用管理プログラム24は、ユーザからパスワードロジックの登録要求が発行されると、ユーザの定義するパスワードロジックを認証用管理ファイル23に登録していくように処理するのである。

【0045】

一方、認証用管理プログラム24は、ユーザから認証用管理ファイル23に登録したパスワードロジックの更新要求が発行されると、図5の処理フローに示すように、先ず最初に、ステップ1で、ディスプレイ装置21に、図8に示したようなパスワードロジック登録画面を表示する。

【0046】

続いて、ステップ2で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザIDを入力し、続くステップ3で、このパスワードロジック登録画面を使ってユーザと対話することで、そのユーザが前回登録したパスワ

ードロジックを入力する。

【0047】

続いて、ステップ4で、ユーザがパスワードロジック登録画面のOKボタン（前回登録したパスワードロジックの入力完了を示すボタン）を操作するのを待って、OKボタンを操作したことを判断するときには、ステップ5に進んで、認証用管理ファイル23を参照することで、そのユーザが前回登録したパスワードロジックを取得する。

【0048】

続いて、ステップ6で、ステップ5で取得したパスワードロジックと、ステップ3で入力したパスワードロジックとが一致するの否かを判断して、一致しないことを判断するときには、前回登録のパスワードロジックを知らなかったことで正規のユーザではないと判断して、パスワードロジックの更新を不許可とすべく、そのまま処理を終了する。

【0049】

一方、ステップ6で、2つのパスワードロジックが一致することを判断するときには、ステップ7に進んで、パスワードロジック登録画面を使ってユーザと対話することで、更新する新たなパスワードロジックを入力する。

【0050】

続いて、ステップ8で、ユーザがパスワードロジック登録画面の終了ボタン（登録実行を指示するボタン）を操作したの否かを判断して、終了ボタンではなくてキャンセルボタンを操作したことを判断するときには、そのまま処理を終了し、終了ボタンを操作したことを判断するときには、ステップ9に進んで、ステップ7で入力した新たなパスワードロジックに従って、認証用管理ファイル23に管理されるそのユーザのパスワードロジックを更新して処理を終了する。

【0051】

このようにして、認証用管理プログラム24は、ユーザからパスワードロジックの更新要求が発行されると、ユーザが認証用管理ファイル23に管理される前回登録したパスワードロジックを知っていることを条件にして、認証用管理ファイル23に管理されるパスワードロジックを更新していくように処理するのであ

る。

【0052】

以上に説明した図4及び図5の処理フローに従って、図3に示したように、認証用管理ファイル23には、ユーザのIDと、そのユーザの登録したパスワードロジック（暗証番号のこともある）との対応関係が登録されることになる。

【0053】

この認証用管理ファイル23の管理データを受けて、ユーザから認証要求要求が発行されると、認証プログラム25は、図6及び7の処理フローに従って、そのユーザの認証処理を実行する。

【0054】

すなわち、認証プログラム25は、ユーザから認証要求が発行されると、図6及び図7の処理フローに示すように、先ず最初に、ステップ1で、数字列“ABCD”で表される4桁の乱数を発生し、続くステップ2で、ディスプレイ装置21に、図9に示すようなパスワード入力画面を表示して、そこに、この発生した乱数をユーザへの提示値として表示する。例えば、“4361”という乱数を発生して、これをパスワード入力画面に表示するのである。

【0055】

続いて、ステップ3で、このパスワード入力画面を使ってユーザと対話することで、ユーザIDとパスワードとを入力する。

【0056】

このときユーザの入力するパスワードは、認証プログラム25の発生した4桁の乱数の持つ数字A／数字B／数字C／数字Dを、そのユーザが認証用管理ファイル23に登録したパスワードロジックに代入することで求められることになる。例えば、認証プログラム25が“4361”という乱数を発生するときに、ユーザが「A+B+C+D」というパスワードロジックを登録しているときには、ユーザは、「4+3+6+1」により求められる“14”というパスワードを求めて、それをパスワード入力画面に入力することになる。

【0057】

このとき、認証プログラム25は、パスワードロジックに分母が“0”となる

割算が存在するときには、その割算結果を“0”として扱うという規約にしているので、ユーザは、その規約に従ってパスワードを算出することになる。また、認証プログラム25は、パスワードロジックに剰余の余る割算が存在するときには、小数点以下を切り捨てるという規約にしているので、ユーザは、その規約に従ってパスワードを算出することになる。また、認証プログラム25は、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約にしているので、ユーザは、その規約に従ってパスワードを算出することになる。

【0058】

また、ユーザは、認証用管理ファイル23に従前通りの暗証番号を登録しているときには、その暗証番号をそのままパスワードとして、パスワード入力画面に入力することになる。

【0059】

このようにして、ステップ3で、ユーザからユーザID及びパスワードを入力すると、続いて、ステップ4で、その入力したユーザIDが認証用管理ファイル23に登録されているのか否かを判断して、登録されていることを判断するときには、ステップ5に進んで、認証用管理ファイル23を参照することで、そのユーザの登録したパスワードロジックを取得する。

【0060】

続いて、ステップ6で、ステップ1で発生した乱数を分解することで、数字A／数字B／数字C／数字Dの値を得る。続いて、ステップ7で、その得た値をステップ5で取得したパスワードロジックに代入することで、ユーザの入力したパスワードに対応する演算値を算出する。

【0061】

このとき、認証プログラム25は、パスワードロジックに分母が“0”となる割算が存在するときには、その割算結果を“0”として扱うという規約に従って演算値を算出し、パスワードロジックに剰余の余る割算が存在するときには、小数点以下を切り捨てるという規約に従って演算値を算出し、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約に従っ

て演算値を算出し、パスワードロジックとして従前通りの暗証番号が登録されているときには、その暗証番号をそのまま演算値として算出していくように処理する。

【0062】

続いて、ステップ8で、ステップ3で入力したパスワードと、ステップ7で算出した演算値とを照合することでユーザ認証処理を実行し、続くステップ9で、その照合により2つのパスワードの一致が検出されたのか否かを判断して、2つのパスワードの一致が検出されるときには、ステップ10に進んで、図示しない業務プログラムに対してユーザ認証完了を出力することで、その業務プログラムに対して処理に入ることを指示する。

【0063】

一方、ステップ4で、入力したユーザIDが認証用管理ファイル23に登録されていないことを判断するときと、ステップ9で、2つのパスワードが一致しないことが検出されるときには、ステップ11（図9の処理フロー）に進んで、ユーザ認証処理を規定回数トライしたのか否かを判断して、規定回数トライしたことを判断するときには、ステップ12に進んで、ディスプレイ装置21に、ユーザ認証エラーを出力して処理を終了する。

【0064】

そして、ステップ11で、ユーザ認証処理を規定回数トライしていないことを判断するときには、ステップ13に進んで、トライ回数を1つカウントアップしてから、ステップ1に戻っていくことで、上述のユーザ認証処理を再度実行していく。

【0065】

このようにして、認証プログラム25は、ユーザから認証要求が発行されると、図6及び図7の処理フローに従って、認証用管理ファイル23に登録されたユーザ定義のパスワードロジックとユーザに提示する乱数とから算出される演算値と、その乱数の提示に応答してユーザが入力してくるパスワードとが一致するの
か否かをチェックしていくことで、ユーザ認証処理を実行するように処理するのである。

【 0 0 6 6 】

このユーザ認証処理に従って、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。そして、ユーザはパスワードロジックのみを覚えれば足りるとともに、システムはパスワードロジックのみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

【 0 0 6 7 】

しかも、従来技術で用いる暗証番号によるユーザ認証処理もそのまま併用できることから、暗証番号を用いたいと希望するユーザの要望にもそのまま対応できることになる。

【 0 0 6 8 】

図 1 0 に、本発明の他の実施例を図示する。

【 0 0 6 9 】

この実施例は、ネットワーク環境で動作する流通管理システムに対して、本発明を適用したものである。

【 0 0 7 0 】

この実施例に従う本発明を具備する流通管理システムは、ユーザ認証処理を実行する認証用サーバ 3 0 と、流通側に設置される複数の流通端末 4 0 と、認証用サーバ 3 0 と流通端末 4 0 との間を接続するネットワーク 5 0 とで構成されている。

【 0 0 7 1 】

この認証用サーバ 3 0 は、図 2 に示した認証用管理ファイル 2 3 と同一のデータを管理する認証用管理ファイル 3 1 と、フロッピーディスクや回線などを介してインストールされて、認証用管理ファイル 3 1 の管理データの登録更新処理を実行する認証用管理プログラム 3 2 と、フロッピーディスクや回線などを介してインストールされて、認証用管理ファイル 3 1 の管理データを使ってユーザ認証処理を実行する認証プログラム 3 3 とを備える。

【 0 0 7 2 】

一方、流通端末 4 0 は、C R T などのディスプレイ装置 4 1 と、マウスなどの

入力装置 42 と、フロッピーディスクや回線などを介してインストールされて、ユーザ認証処理のための対話処理を実行する対話プログラム 43 とを備える。

【0073】

図 11/図 13/図 14/図 17 に、対話プログラム 43 の実行する処理フローの一実施例、図 12/図 15/図 16 に、認証用管理プログラム 32 の実行する処理フローの一実施例、図 18 に、認証プログラム 33 の実行する処理フローの一実施例を図示する。次に、これらの処理フローに従って、図 10 のように構成される実施例の処理について説明する。

【0074】

先ず最初に、図 11 及び図 12 の処理フローに従って、認証用管理ファイル 31 に対するパスワードロジックの登録処理について説明する。

【0075】

流通端末 40 に展開される対話プログラム 43 は、ユーザから認証用管理ファイル 31 に対するパスワードロジックの登録要求が発行されると、図 11 の処理フローに示すように、先ず最初に、ステップ 1 で、ディスプレイ装置 41 に、図 8 に示したようなパスワードロジック登録画面を表示する。

【0076】

続いて、ステップ 2 で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザ ID を入力し、続くステップ 3 で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザの定義するパスワードロジック（図 2 の実施例で入力したパスワードロジックと同じもの）を入力する。

【0077】

続いて、ステップ 4 で、ユーザがパスワードロジック登録画面の終了ボタン（登録実行を指示するボタン）を操作したのか否かを判断して、終了ボタンではなくてキャンセルボタンを操作したことを判断するときには、そのまま処理を終了し、終了ボタンを操作したことを判断するときには、ステップ 5 に進んで、入力したユーザ ID とパスワードロジックとを認証用管理プログラム 32 に送信する。

【0078】

後述するように、認証用管理プログラム 32 は、この送信に応答して、対話プログラム 43 の送信したパスワードロジックの登録ができたのか否かを示す情報を返信してくるので、続いて、ステップ 6 で、認証用管理プログラム 32 からの返信情報を待って、この返信情報を受け取ると、続くステップ 7 で、この返信情報がパスワードロジックの登録完了を示す情報であるのか否かを判断する。

【0079】

この判断処理に従って、認証用管理プログラム 32 からパスワードロジックの登録完了を示す情報が返信されてきたことを判断するときには、そのまま処理を終了し、登録できない旨の情報が返信されてきたことを判断するときには、ステップ 8 に進んで、ディスプレイ装置 41 に、パスワードロジックを登録できない旨を出力して処理を終了する。

【0080】

この図 11 の処理フローで示した対話プログラム 43 の処理を受けて、認証用サーバ 30 に展開される認証用管理プログラム 32 は、対話プログラム 43 がパスワードロジックの登録要求を発行すると、図 12 の処理フローに示すように、先ず最初に、ステップ 1 で、対話プログラム 43 から送られてくるユーザ ID と登録要求のパスワードロジックとを受け取る。

【0081】

続いて、ステップ 2 で、その受け取ったユーザ ID の指すユーザのパスワードロジックが既に認証用管理ファイル 31 に登録されているのか否かを判断して、既に登録されていることを判断するときには、ステップ 3 に進んで、対話プログラム 43 に対して、登録要求のパスワードロジックを登録できない旨を返信して処理を終了する。

【0082】

一方、ステップ 2 で、受け取ったユーザ ID の指すユーザのパスワードロジックが認証用管理ファイル 31 に登録されていないことを判断するときには、ステップ 4 に進んで、受け取った登録要求のパスワードロジックを受け取ったユーザ ID と対応をとりつつ、認証用管理ファイル 31 に登録し、続くステップ 5 で、対話プログラム 43 に対して、登録要求のパスワードロジックの登録を完了した

旨を返信して処理を終了する。

【0083】

このようにして、対話プログラム43と認証用管理プログラム32とは、ユーザからパスワードロジックの登録要求が発行されると、ネットワーク50を介して連携処理を実行しつつ、ユーザの定義するパスワードロジックを認証用管理ファイル31に登録していくように処理するのである。

【0084】

次に、図13ないし図16の処理フローに従って、認証用管理ファイル31に管理されるパスワードロジックの更新処理について説明する。

【0085】

流通端末40に展開される対話プログラム43は、ユーザから認証用管理ファイル31に登録したパスワードロジックの更新要求が発行されると、図13の処理フローに示すように、先ず最初に、ステップ1で、ディスプレイ装置41に、図8に示したようなパスワードロジック登録画面を表示する。

【0086】

続いて、ステップ2で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザIDを入力し、続くステップ3で、このパスワードロジック登録画面を使ってユーザと対話することで、そのユーザが前回登録したパスワードロジックを入力する。

【0087】

続いて、ステップ4で、ユーザがパスワードロジック登録画面のOKボタン（前回登録したパスワードロジックの入力完了を示すボタン）を操作するのを待って、OKボタンを操作したことを判断するときには、ステップ5に進んで、入力したユーザIDとパスワードロジック（ユーザが前回登録したもの）とを認証用管理プログラム32に送信する。

【0088】

後述するように、認証用管理プログラム32は、この送信に応答して、対話プログラム43の発行するパスワードロジックの更新要求が実行できるのか否かを示す情報を返信してくるので、続いて、ステップ6で、認証用管理プログラム3

2からの返信情報を待って、この返信情報を受け取ると、続くステップ7で、この返信情報がパスワードロジックの更新の可能を示す情報であるのか否かを判断する。

【0089】

この判断処理に従って、認証用管理プログラム32からパスワードロジックの更新不可能を示す情報が返信されてきたことを判断するときには、ステップ8に進んで、ディスプレイ装置41に、パスワードロジックを更新できない旨を出力して処理を終了する。

【0090】

一方、ステップ7で、認証用管理プログラム32からパスワードロジックの更新可能を示す情報が返信されてきたことを判断するときには、ステップ9に進んで、パスワードロジック登録画面を使ってユーザと対話することで、更新する新たなパスワードロジックを入力する。

【0091】

続いて、ステップ10（図14の処理フロー）で、ユーザがパスワードロジック登録画面の終了ボタン（登録実行を指示するボタン）を操作したのか否かを判断して、終了ボタンではなくてキャンセルボタンを操作したことを判断するときには、そのまま処理を終了し、終了ボタンを操作したことを判断するときには、ステップ11に進んで、ユーザIDとステップ9で入力したパスワードロジック（更新要求のもの）とを認証用管理プログラム32に送信する。

【0092】

後述するように、認証用管理プログラム32は、この送信に応答して、対話プログラム43の送信したパスワードロジックの登録ができたことを示す情報を返信してくるので、続いて、ステップ12で、認証用管理プログラム32からの返信情報を待って、この返信情報を受け取ると、処理を終了する。

【0093】

この図13及び図14の処理フローに示した対話プログラム43の処理を受けて、認証用サーバ30に展開される認証用管理プログラム32は、対話プログラム43がパスワードロジックの更新要求を発行すると、図15及び図16の処理

フローに示すように、先ず最初に、ステップ1で、対話プログラム43から送られてくるユーザIDと前回登録のパスワードロジックとを受け取る。

【0094】

続いて、ステップ2で、認証用管理ファイル31を参照することで、その受け取ったユーザIDの指すパスワードロジックを取得する。続いて、ステップ3で、ステップ2で取得したパスワードロジックと、ステップ1で受け取ったパスワードロジックとが一致するの否かを判断して、一致しないことを判断するときには、ステップ4に進んで、対話プログラム43に対して、パスワードロジックを更新できない旨を返信して処理を終了する。

【0095】

一方、ステップ3で、2つのパスワードロジックが一致することを判断するときには、ステップ5に進んで、対話プログラム43に対して、パスワードロジックを更新できる旨を返信する。

【0096】

上述したように、対話プログラム43は、認証用管理プログラム32からパスワードロジックの更新が可能である旨の通知を受け取ると、ユーザIDと更新要求のパスワードロジックとを送信してくるので、続いて、ステップ6で、対話プログラム43から、ユーザIDと更新要求のパスワードロジックとが送られてくるのを待って、それを受け取る。

【0097】

続いて、ステップ7（図16の処理フロー）で、その受け取った更新要求のパスワードロジックに従って、認証用管理ファイル31に管理されるその受け取ったユーザIDの指すパスワードロジックを更新し、続くステップ8で、対話プログラム43に対して、パスワードロジックの更新完了を通知して処理を終了する。

【0098】

このようにして、対話プログラム43と認証用管理プログラム32とは、ユーザからパスワードロジックの更新要求が発行されると、ネットワーク50を介して連携処理を実行しつつ、ユーザが前回登録のパスワードロジックを知っている

ことを条件にして、認証用管理ファイル 31 に管理されるパスワードロジックを更新していくように処理するのである。

【0099】

以上に説明した図 11 ないし図 16 の処理フローに従って、図 3 に示したように、認識用サーバ 30 の備える認証用管理ファイル 31 には、ユーザの ID と、そのユーザの登録したパスワードロジック（暗証番号のこともある）との対応関係が登録されることになる。

【0100】

この認証用管理ファイル 31 の管理データを受けて、ユーザから認証要求が発行されると、対話プログラム 43 と認証用管理プログラム 32 とは、ネットワーク 50 を介して連携処理を実行しつつ、そのユーザの認証処理を実行する。

【0101】

次に、図 17 及び図 18 の処理フローに従って、このとき実行されるユーザ認証処理について説明する。

【0102】

流通端末 40 に展開される対話プログラム 43 は、ユーザからユーザ認証処理の実行要求が発行されると、図 17 の処理フローに示すように、先ず最初に、ステップ 1 で、数字列“ABCD”で表される 4 桁の乱数を発生し、続くステップ 2 で、ディスプレイ装置 41 に、図 9 に示したようなパスワード入力画面を表示して、そこに、この発生した乱数をユーザへの提示値として表示する。例えば、“4361”という乱数を発生して、これをパスワード入力画面に表示するのである。

【0103】

なお、後述することからも分かるように、このとき発生する乱数は 4 桁である必要はなく、1 桁や 2 桁や 3 桁であってもよく、更に大きな桁数であってもよい。

【0104】

続いて、ステップ 3 で、このパスワード入力画面を使ってユーザと対話することとで、ユーザ ID とパスワードとを入力する。

【0105】

このときユーザの入力するパスワードは、対話プログラム43の発生した4桁の乱数の持つ数字A／数字B／数字C／数字Dを、そのユーザが認証用管理ファイル41に登録したパスワードロジックに代入することで求められることになる。このとき、ユーザは、パスワードロジックに分母が“0”となる割算が存在するときには、その割算結果を“0”として算出するという規約に従ってパスワードを算出し、パスワードロジックに剰余のする割算が存在するときには、小数点以下を切り捨てるという規約に従ってパスワードを算出し、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約に従ってパスワードを算出することになる。また、ユーザは、認証用管理ファイル41に従前通りの暗証番号に登録しているときには、その暗証番号をそのままパスワードとして、パスワード入力画面に入力することになる。

【0106】

このようにして、ステップ3で、ユーザID及びパスワードを入力すると、続いて、ステップ4で、ステップ1で発生した乱数と、ステップ3で入力したユーザID／パスワードとを認証プログラム33に送信する。

【0107】

後述するように、認証プログラム33は、この送信に回答して、対話プログラム43の発行するパスワードに従ってユーザを認証できたのか否かを示す情報を返信してくるので、続いて、ステップ5で、認証プログラム33からの返信情報を待って、この返信情報を受け取ると、続くステップ6で、この返信情報がユーザ認証の完了を示す情報であるのか否かを判断する。

【0108】

この判断処理に従って、認証プログラム33からユーザ認証の完了を示す情報が返信されてきたことを判断するときには、ステップ7に進んで、図示しない業務プログラムに対してユーザ認証完了を出力することで、その業務プログラムに対して処理に入ることを指示する。

【0109】

一方、ステップ6で、認証プログラム33からユーザ認証の不可能を示す情報

が返信されてきたことを判断するときには、ステップ8に進んで、ユーザ認証処理を規定回数トライしたのか否かを判断して、ユーザ認証処理を規定回数トライしたことを判断するときには、ステップ9に進んで、ディスプレイ装置41に、ユーザ認証エラーを出力して処理を終了する。

【0110】

そして、ステップ8で、ユーザ認証処理を規定回数トライしていないことを判断するときには、ステップ10に進んで、トライ回数を1つカウントアップしてから、ステップ1に戻っていくことで、上述のユーザ認証処理を再度実行していく。

【0111】

この図17の処理フローに示した対話プログラム43の処理を受けて、認証用サーバ30に展開される認証プログラム33は、対話プログラム43がユーザ認証処理の実行要求を発行すると、図18の処理フローに示すように、先ず最初に、ステップ1で、対話プログラム43から送られてくる、乱数とユーザIDとパスワードロジックとを受け取る。

【0112】

続いて、ステップ2で、その受け取ったユーザIDが認証用管理ファイル31に登録されているのか否かを判断して、登録されていることを判断するときには、ステップ3に進んで、認証用管理ファイル31を参照することで、そのユーザIDの指すパスワードロジックを取得する。

【0113】

続いて、ステップ4で、ステップ1で受け取った乱数を分解することで、数字A/数字B/数字C/数字Dの値を得る。続いて、ステップ5で、その得た値をステップ3で取得したパスワードロジックに代入することで、ユーザの入力したパスワードに対応する演算値を算出する。

【0114】

このとき、認証プログラム33は、パスワードロジックに分母が“0”となる割算が存在するときには、その割算結果を“0”として扱うという規約に従って演算値を算出し、パスワードロジックに剰余のする割算が存在するときには、小

数点以下を切り捨てるという規約に従って演算値を算出し、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約に従って演算値を算出し、パスワードロジックとして従前通りの暗証番号が登録されているときには、その暗証番号をそのまま演算値として算出していくように処理する。

【0115】

続いて、ステップ6で、ステップ1で受け取ったパスワードと、ステップ5で算出した演算値とを照合することでユーザ認証処理を実行し、続くステップ7で、その照合により2つのパスワードの一致が検出されたのか否かを判断して、2つのパスワードの一致が検出されるときには、ステップ8に進んで、対話プログラム43に対してユーザ認証完了を返信して、処理を終了する。

【0116】

一方、ステップ2で、対話プログラム43から受け取ったユーザIDが認証用管理ファイル31に登録されていないことを判断するときと、ステップ7で、2つのパスワードが一致しないことが検出されるときには、ステップ9に進んで、対話プログラム43に対してユーザ認証エラーを返信して、処理を終了する。

【0117】

このようにして、対話プログラム43と認証プログラム33とは、ユーザから認証要求要求が発行されると、図17及び図18の処理フローに従って、ネットワーク50を介して連携処理を実行しつつ、認証用管理ファイル32に登録されたユーザ定義のパスワードロジックとユーザに提示する乱数とから算出される演算値と、その乱数の提示に応答してユーザが入力してくるパスワードとが一致するのか否かをチェックしていくことで、ユーザ認証処理を実行するように処理するのである。

【0118】

このユーザ認証処理に従って、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。そして、ユーザはパスワードロジックのみを覚えれば足りるとともに、システムはパスワードロジックのみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけ

ることなく高いセキュリティを実現できるようになる。

【0119】

更に、暗証番号に相当するパスワードロジックについては、それが認証用管理ファイル32に登録される場合を除きネットワーク50に転送されることがないことで盗み見られるという危険性がなく、これにより高いセキュリティを実現できるようになる。

【0120】

ここで、図17及び図18の処理フローでは、対話プログラム43が乱数を発生していく構成を採ったが、認証プログラム33が乱数を発生して、それを対話プログラム43に通知していくという構成を採ることも可能である。

【0121】

以上に説明したように、本発明は、ユーザ定義のパスワードロジックを登録し、乱数を発生してユーザに提示する構成を採って、暗証番号の代わりに、その乱数の提示に応答してユーザから入力される数値と、そのパスワードロジックとその乱数とから算出される数値との一致をチェックしていくことでユーザ認証を実行する構成を採ることを、基本的な技術思想としている。

【0122】

この技術思想に従って、本発明では、磁気カードやICカードなどのようなユーザ認証用カードに、暗証番号に代えて、上述したようなユーザ定義のパスワードロジックを記録していく構成を採ることになる。

【0123】

すなわち、従来の磁気カードやICカードなどのユーザ認証用カードでは、ユーザIDと暗証番号とを記録する構成を採るのに対して、本発明を具備するユーザ認証用カードでは、ユーザIDとユーザ定義のパスワードロジックとを記録する構成を採ることになる。

【0124】

図19に、本発明を具備するICカード60の一実施例を図示する。

【0125】

この図に示すように、本発明を具備するICカード60は、メモリ部600に

、ユーザIDとユーザ定義のパスワードロジックとを記録するとともに、乱数発生機構601を備える構成を採る。

【0126】

このように構成される本発明を具備するICカード60は、流通端末40の備えるICカードリーダー70にセットされ、一方、流通端末40には、このICカード60に記録されるパスワードロジックを使って、ユーザ認証処理を実行するカード認証プログラム44が備えられることになる。

【0127】

図20及び図21に、このカード認証プログラム44の実行する処理フローの一実施例を図示する。次に、この処理フローに従って、本発明を具備するICカード60に適用されるユーザ認証処理について説明する。

【0128】

流通端末40に展開されるカード認証プログラム44は、本発明を具備するICカード60に対するユーザ認証要求が発行されると、図20及び図21の処理フローに示すように、先ず最初に、ステップ1で、ICカード60に記録されるユーザIDとパスワードロジックとを読み取る。

【0129】

続いて、ステップ2で、ICカード60の乱数発生機構601が発生する4桁の乱数を入力する。続いて、ステップ3で、図9に示すようなパスワード入力画面を表示して、そこに、この入力した乱数をユーザへの提示値として表示する。例えば、“4361”という乱数が発生して、これをパスワード入力画面に表示するのである。

【0130】

続いて、ステップ4で、このパスワード入力画面を使ってユーザと対話することで、パスワードを入力する。

【0131】

このときユーザの入力するパスワードは、乱数発生機構601の発生した4桁の乱数の持つ数字A／数字B／数字C／数字Dを、ICカード60に記録されるパスワードロジックに代入することで求められることになる。このとき、ユーザ

は、パスワードロジックに分母が“0”となる割算が存在するときには、その割算結果を“0”として算出するという規約に従ってパスワードを算出し、パスワードロジックに剰余のする割算が存在するときには、小数点以下を切り捨てるという規約に従ってパスワードを算出し、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約に従ってパスワードを算出することになる。また、ユーザは、ICカード60が従前通りの暗証番号を記録しているときには、その暗証番号をそのままパスワードとして、パスワード入力画面に入力することになる。

【0132】

このようにして、ステップ4で、ユーザからパスワードを入力すると、続いて、ステップ5で、ステップ1で読み取った乱数を分解することで、数字A/数字B/数字C/数字Dの値を得る。続いて、ステップ6で、その得た値をステップ1で読み取ったパスワードロジックに代入することで、ユーザの入力したパスワードに対応する演算値を算出する。

【0133】

続いて、ステップ7で、ステップ4で入力したパスワードと、ステップ6で算出した演算値とを照合することでユーザ認証処理を実行し、続くステップ8で、その照合により2つのパスワードの一致が検出されたのか否かを判断して、2つのパスワードの一致が検出されるときには、ステップ9に進んで、図示しない業務プログラムに対してユーザ認証完了を出力することで、その業務プログラムに対して処理に入ることを指示する。

【0134】

一方、ステップ8で、2つのパスワードが一致しないことが検出されるときには、ステップ10に進んで、ユーザ認証処理を規定回数トライしたのか否かを判断して、ユーザ認証処理を規定回数トライしたことを判断するときには、ステップ11（図21の処理フロー）に進んで、ディスプレイ装置41に、ユーザ認証エラーを出力して処理を終了する。

【0135】

そして、ステップ10で、ユーザ認証処理を規定回数トライしていないことを

判断するときには、ステップ 12（図 21 の処理フロー）に進んで、トライ回数を 1 つカウントアップしてから、ステップ 1 に戻っていくことで、上述のユーザ認証処理を再度実行していく。

【0136】

このようにして、本発明では、磁気カードや IC カードなどのようなユーザ認証用カードに、暗証番号に代えて、上述したようなユーザ定義のパスワードロジックを記録する構成を採る。そして、ユーザ認証用カードに記録されたユーザ定義のパスワードロジックとユーザに提示する乱数とから算出される演算値と、その乱数の提示に応答してユーザが入力してくるパスワードとが一致するのか否かをチェックしていくことで、ユーザ認証処理を実行するように処理するのである。

【0137】

このユーザ認証処理に従って、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。

【0138】

なお、図 19 に示した実施例では、IC カード 60 に乱数発生機構 601 を備える構成を採ったが、この乱数発生機能については、カード認証プログラム 44 の方に備えるという構成を採ることも可能である。

【0139】

以上に説明した実施例では、乱数の持つ数字に対する四則演算で定義されるパスワードロジックを開示したが、この乱数の持つ数字の他に、カレンダー情報や時刻情報などのような全ユーザ及びシステムが一義的に決定できる変数値を含めることも可能である。

【0140】

例えば、1 月～12 月に対して、“1”～“12”という変数値 n を割り付けたり、0 時～24 時に対して、“0”～“24”という変数値 n を割り付けたりして、例えば、「 $(A-B) + n$ 」というように、乱数の持つ数字の他に、この変数値 n を含める形でパスワードロジックを定義することも可能である。

【0141】

【発明の効果】

以上説明したように、本発明では、ユーザ定義の計算式を登録し、乱数を発生してユーザに提示する構成を採って、暗証番号の代わりに、その乱数の提示に回答してユーザから入力される数値と、その計算式とその乱数とから算出される数値との一致をチェックしていくことでユーザ認証を実行する構成を採ることから、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。

【0142】

そして、ネットワーク環境で使用される場合に、ユーザ定義の計算式を転送しない構成を採ることで、暗証番号を転送する従来技術に比べて、高いセキュリティを実現できるようになる。

【0143】

しかも、特開昭63-170764号で開示されたユーザ認証技術に従うと、ユーザは計算式と固有値との両方を覚えなくてはならないのに対して、本発明では、ユーザは計算式のみを覚えれば足りるとともに、特開昭63-170764号で開示されたユーザ認証技術に従うと、システムは計算式と固有値との両方をメモリに記憶しなければならないのに対して、本発明では、システムは計算式のみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

【0144】

そして、本発明では、カードの所有者の認証用に用意されるカードに、暗証番号に代えて、ユーザ定義の計算式を記録する構成を採ることで、従来技術よりも高いセキュリティを実現できるようになる。

【図面の簡単な説明】

【図1】

本発明の原理構成図である。

【図2】

本発明の一実施例である。

【図3】

認証用管理ファイルの一実施例である。

【図 4】

認証用管理プログラムの処理フローである。

【図 5】

認証用管理プログラムの処理フローである。

【図 6】

認証プログラムの処理フローである。

【図 7】

認証プログラムの処理フローである。

【図 8】

パスワードロジック登録画面の一実施例である。

【図 9】

パスワード入力画面の一実施例である。

【図 1 0】

本発明の他の実施例である。

【図 1 1】

対話プログラムの処理フローである。

【図 1 2】

認証用管理プログラムの処理フローである。

【図 1 3】

対話プログラムの処理フローである。

【図 1 4】

対話プログラムの処理フローである。

【図 1 5】

認証用管理プログラムの処理フローである。

【図 1 6】

認証用管理プログラムの処理フローである。

【図 1 7】

対話プログラムの処理フローである。

【図 18】

認証プログラムの処理フローである。

【図 19】

本発明の一実施例である。

【図 20】

カード認証プログラムの処理フローである。

【図 21】

カード認証プログラムの処理フローである。

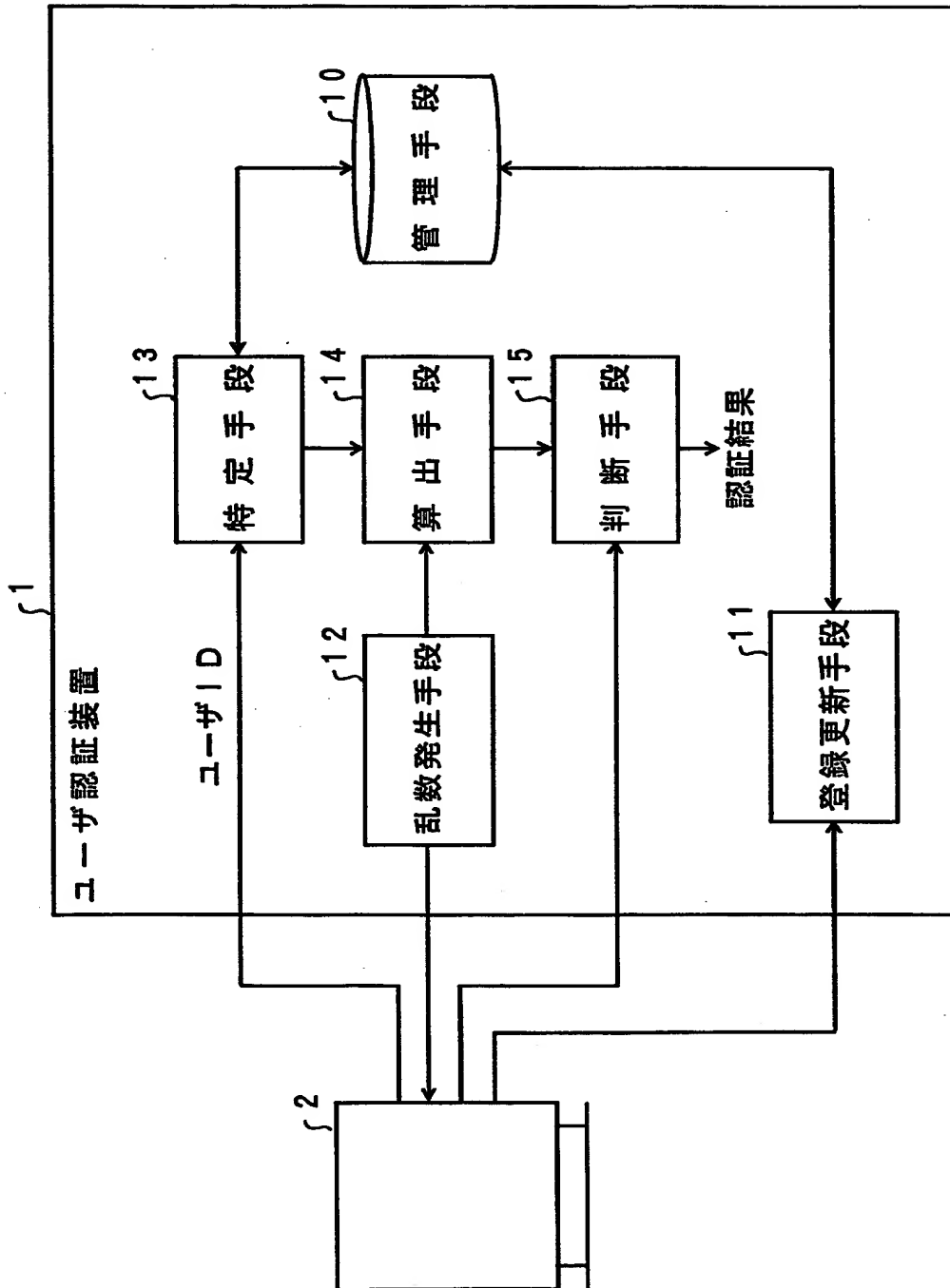
【符号の説明】

- 1 ユーザ認証装置
- 2 端末
- 10 管理手段
- 11 登録更新手段
- 12 乱数発生手段
- 13 特定手段
- 14 算出手段
- 15 判断手段

【書類名】 図面

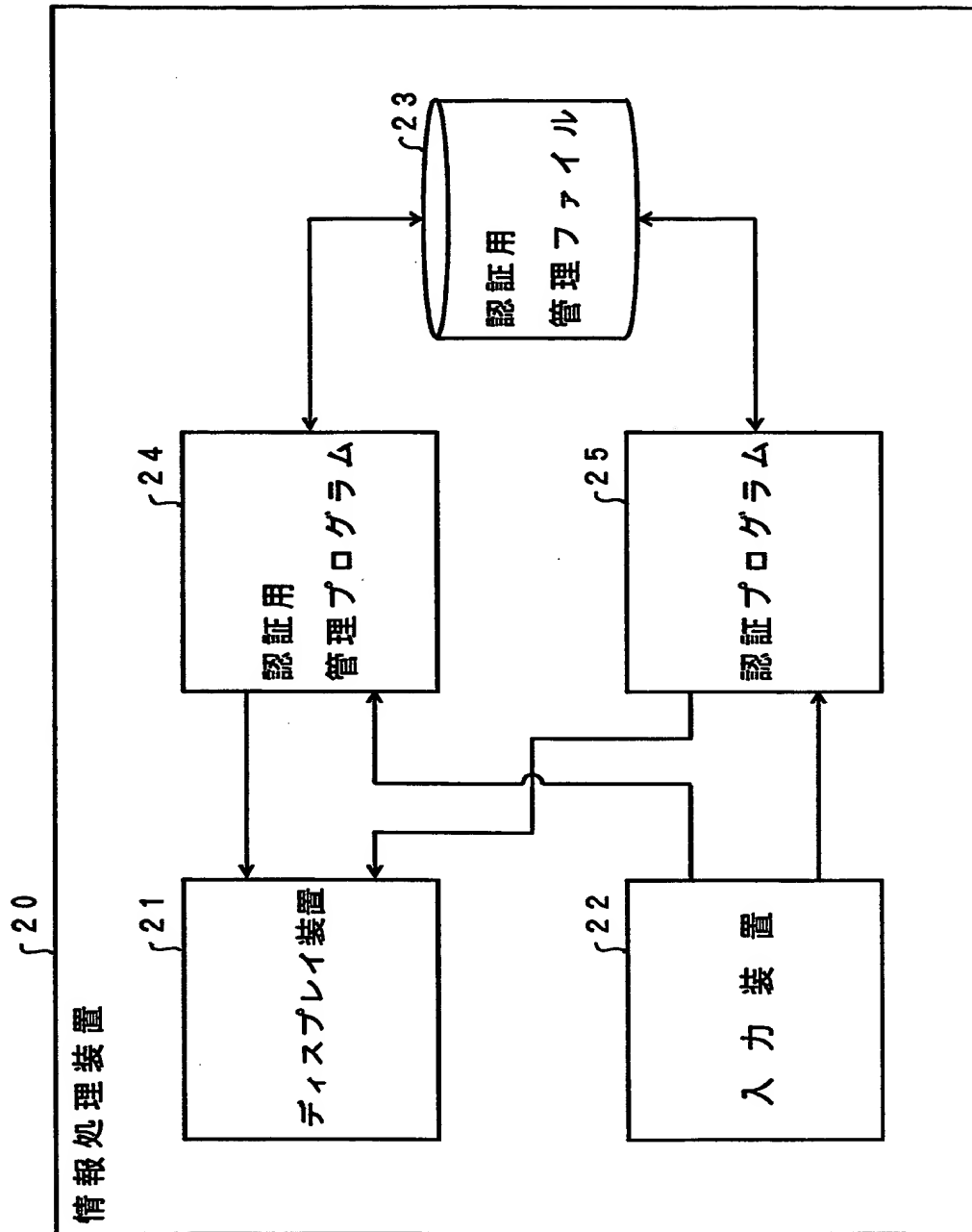
【図 1】

本 発 明 の 原 理 構 成 図



【図 2】

本 発 明 の 一 実 施 例



【図 3】

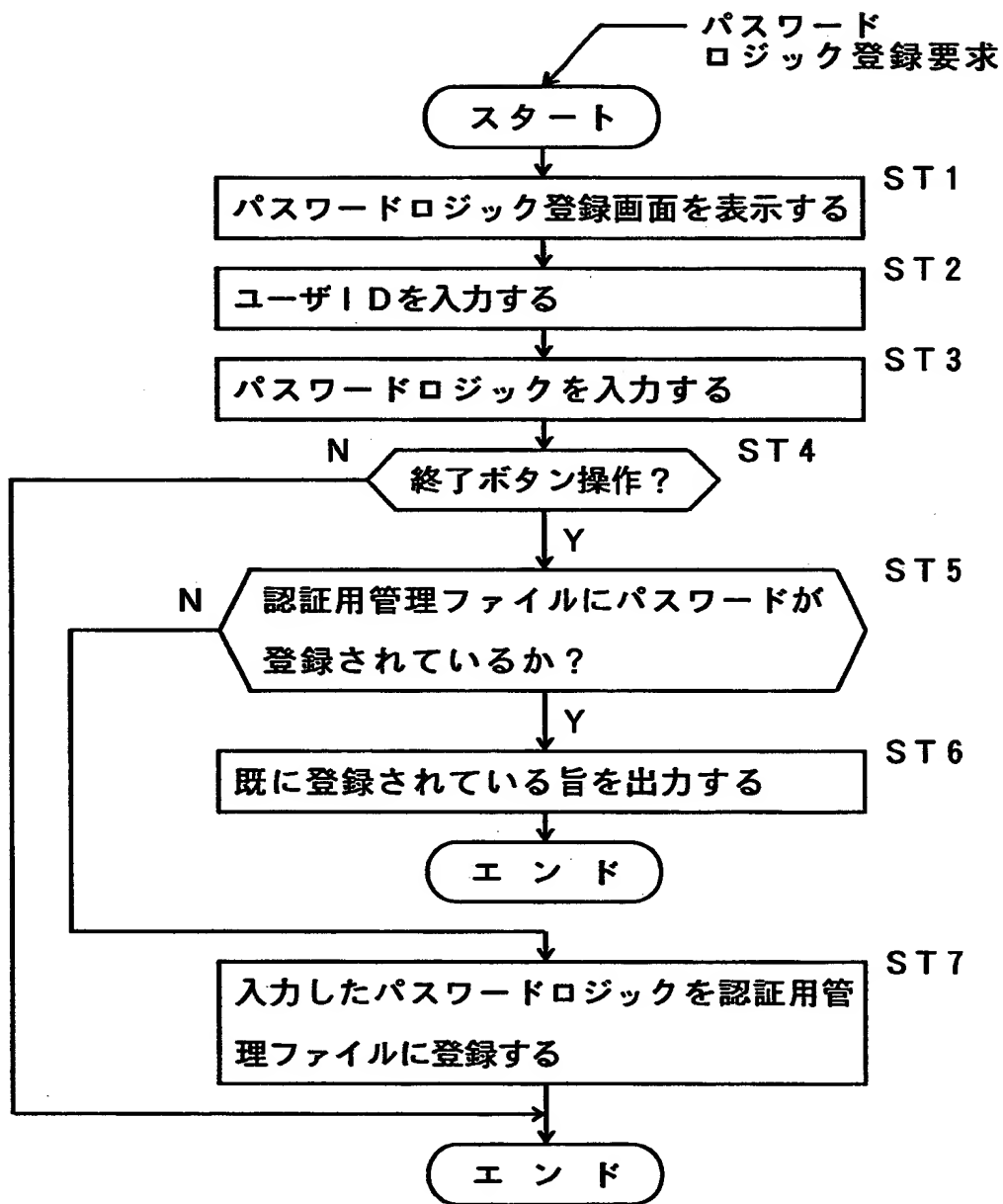
認 証 用 管 理 フ ァ イ ル の 一 実 施 例

23

ユーザID	パスワードロジック
000001	$10 \times A$
000002	$A \times A$
000003	$A \div B$
000004	5384
000005	$A - B$
000006	$(B - A) + C$
000007	$((A - B) \times 5) \div 2$
•	•
•	•
•	•
•	•
•	•

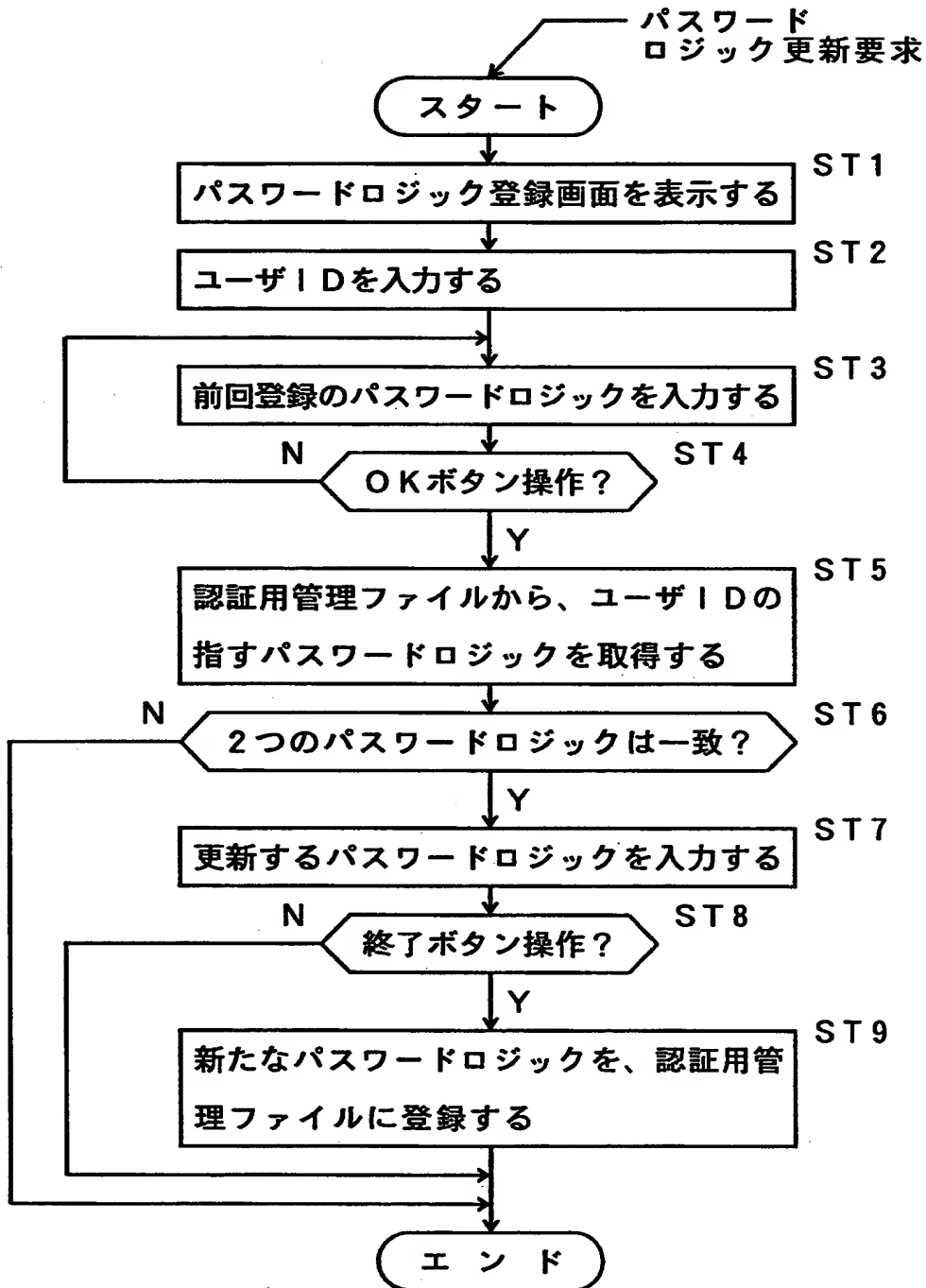
【図 4】

認証用管理プログラムの処理フロー



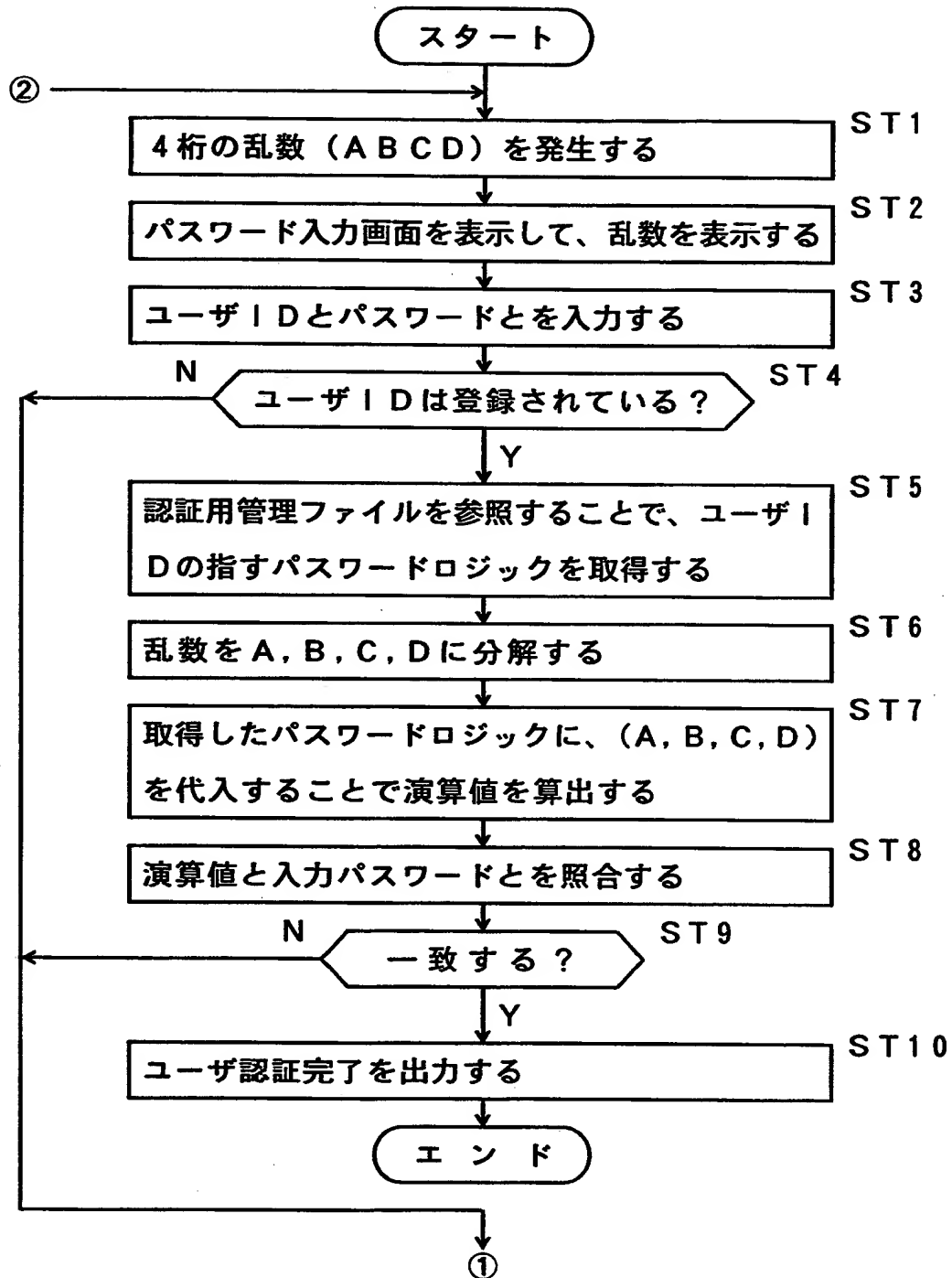
【図5】

認証用管理プログラムの処理フロー



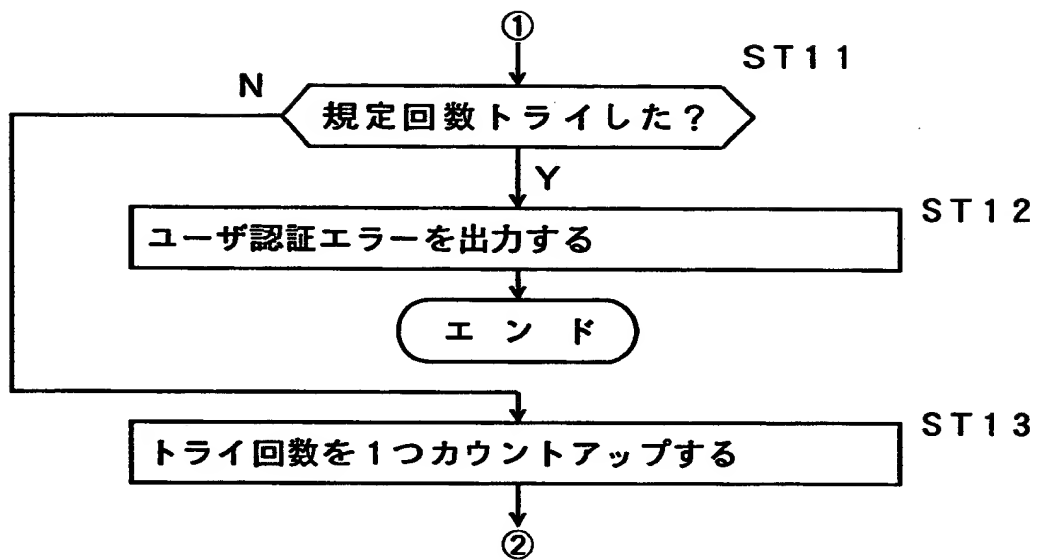
【図 6】

認証プログラムの処理フロー



【図7】

認証プログラムの処理フロー



【図 8】

パスワードロジック登録画面の一実施例

パスワードロジック登録		
ユーザID	:	000006
パスワードロジック	:	$(B-A)+C$
OK		キャンセル
		終了

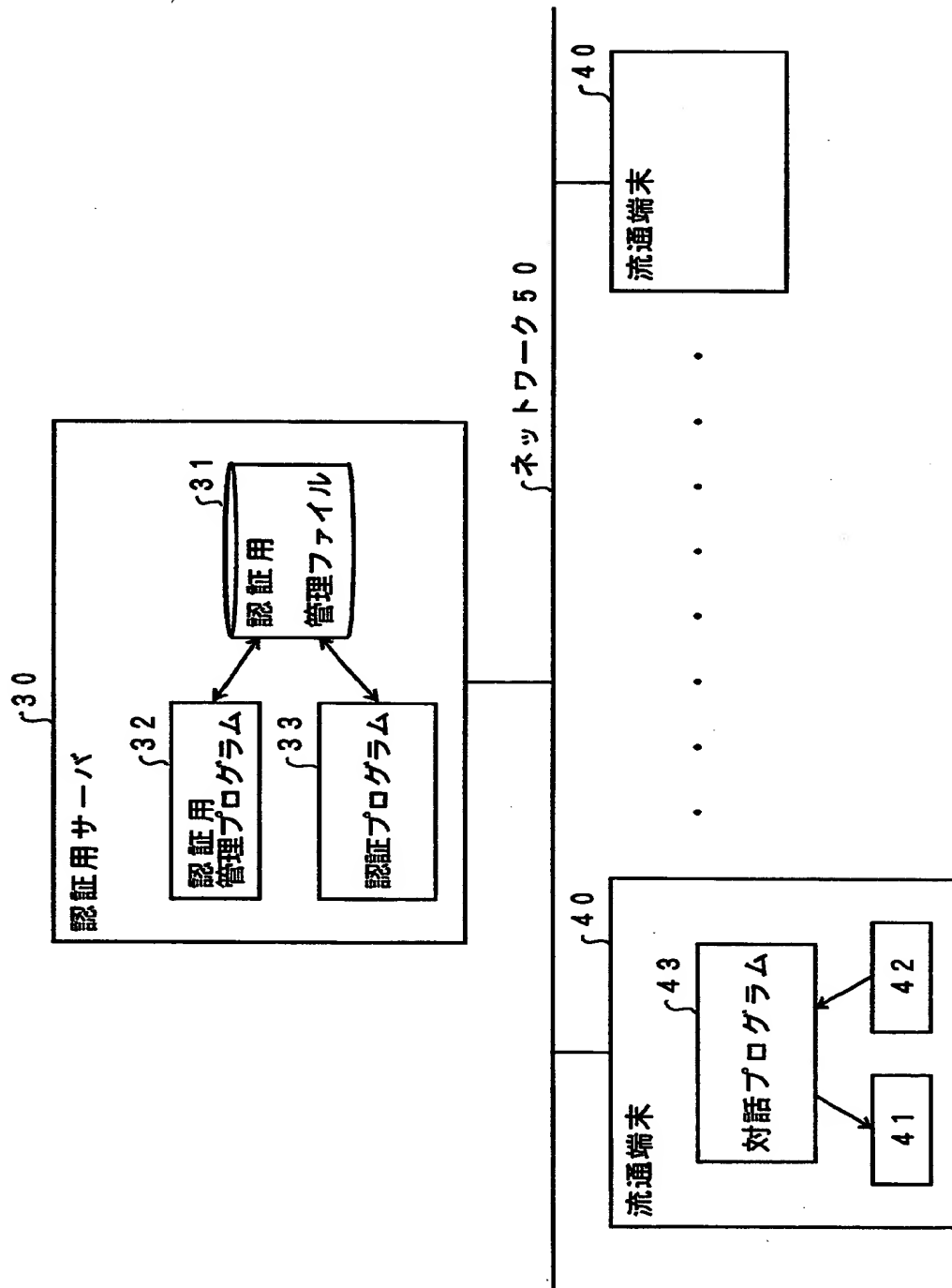
【図9】

パスワード入力画面の実施例

パスワード入力		
ユーザID	:	000001
提示値	:	4361
パスワード	:	**
OK		キャンセル
		終了

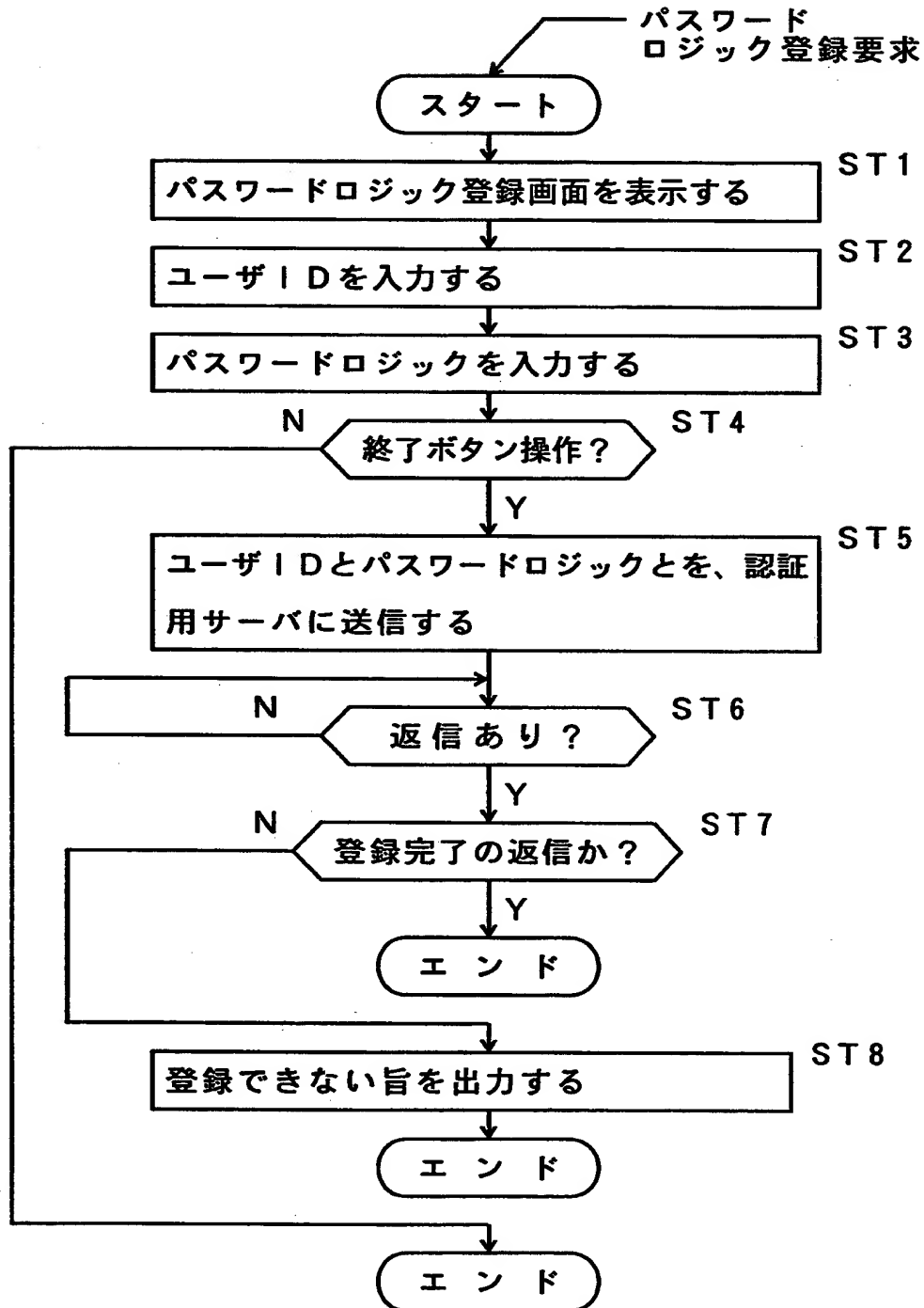
【図10】

本 発 明 の 他 の 実 施 例



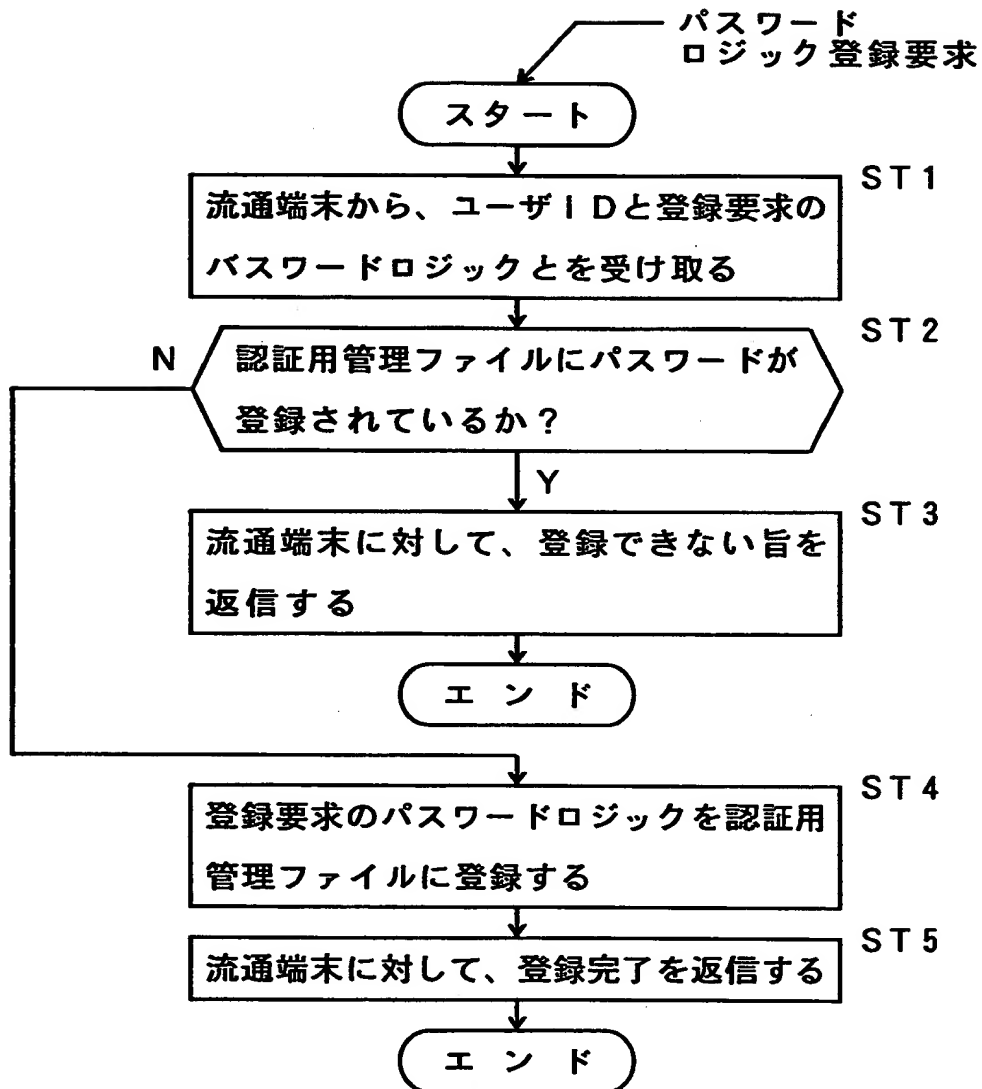
【図 11】

対話プログラムの処理フロー



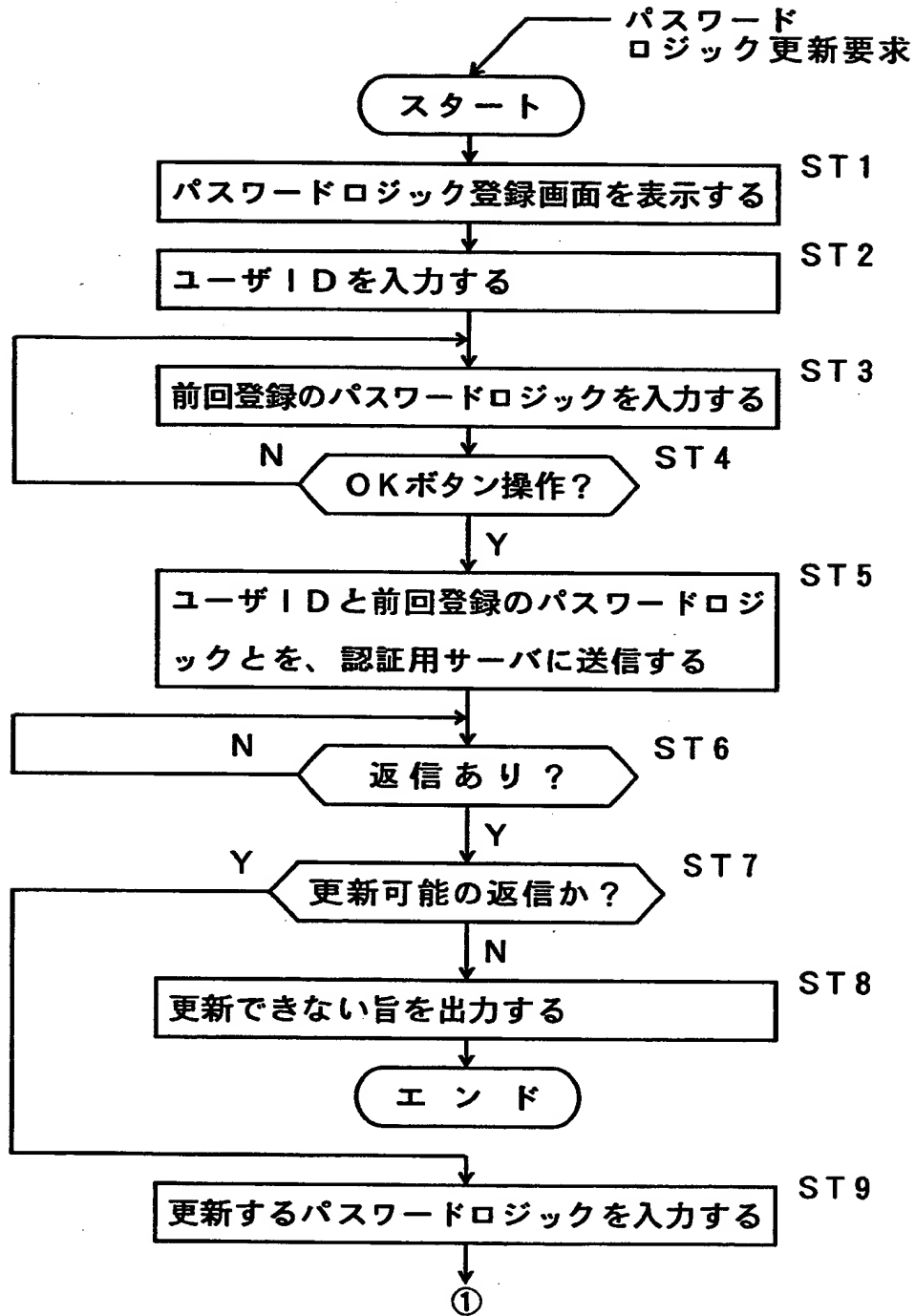
【図 12】

認証用管理プログラムの処理フロー



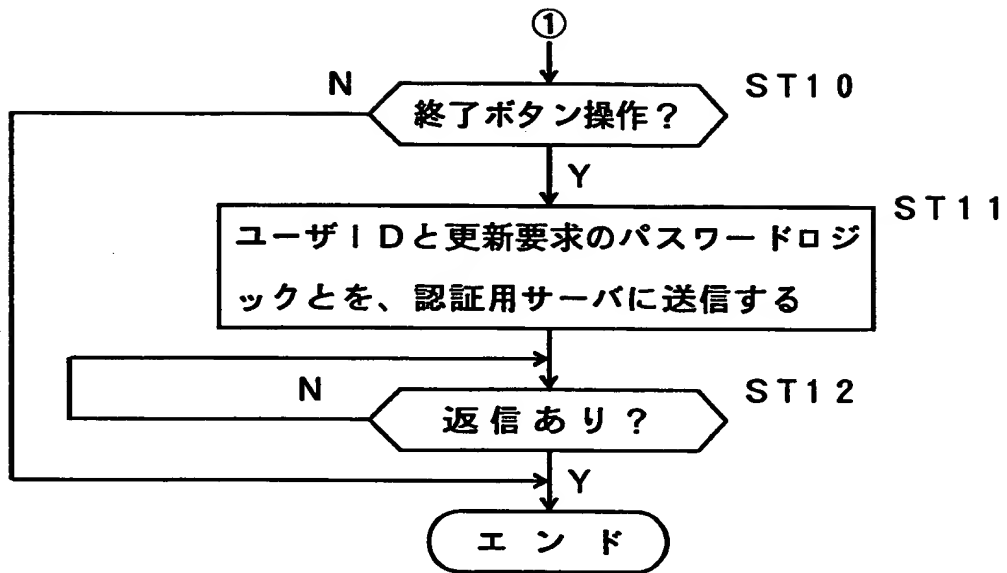
【図 13】

対話プログラムの処理フロー



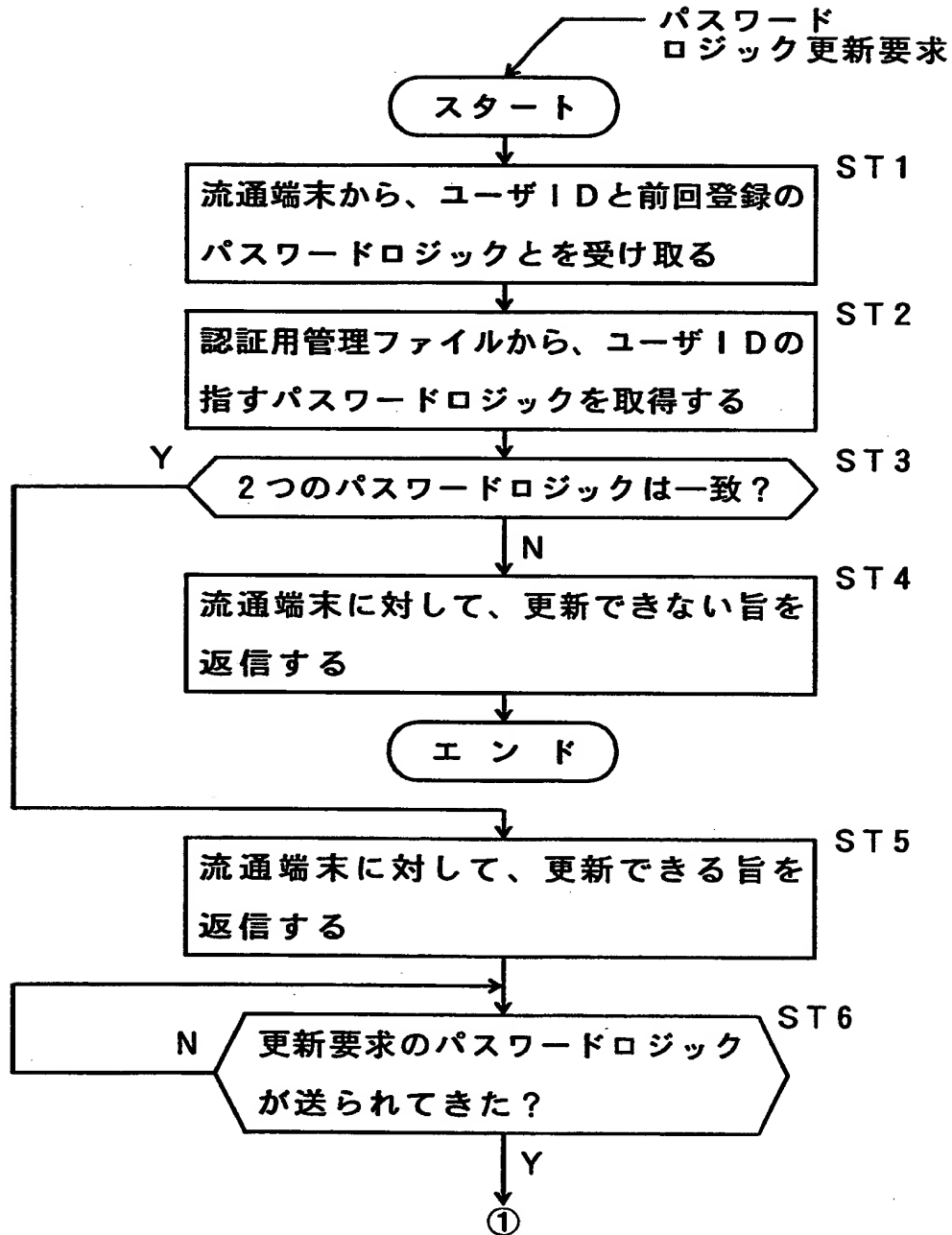
【図 14】

対 話 プ ロ グ ラ ム の 処 理 フ ロ ー



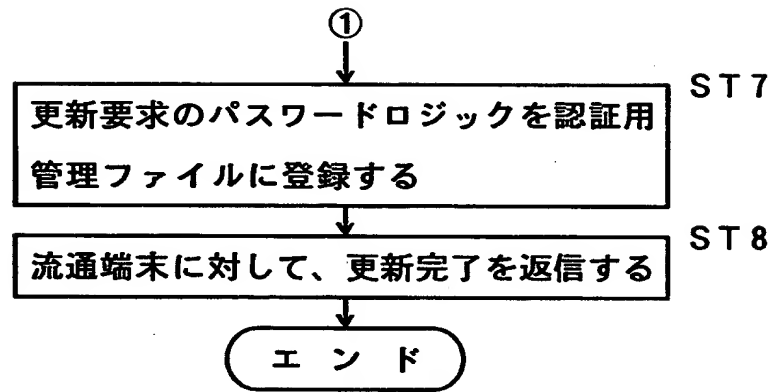
【図 15】

認証用管理プログラムの処理フロー



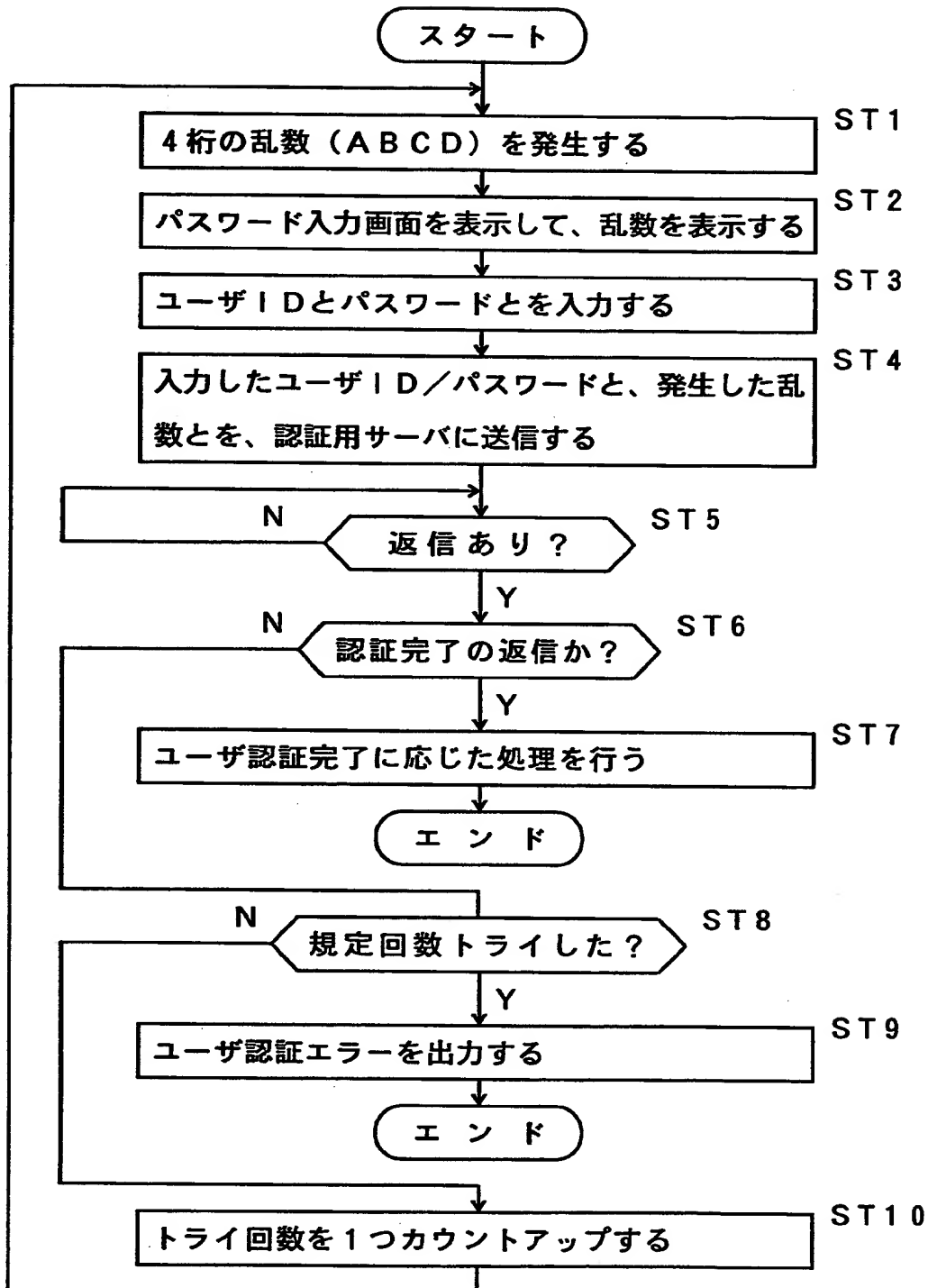
【図 16】

認証用管理プログラムの処理フロー



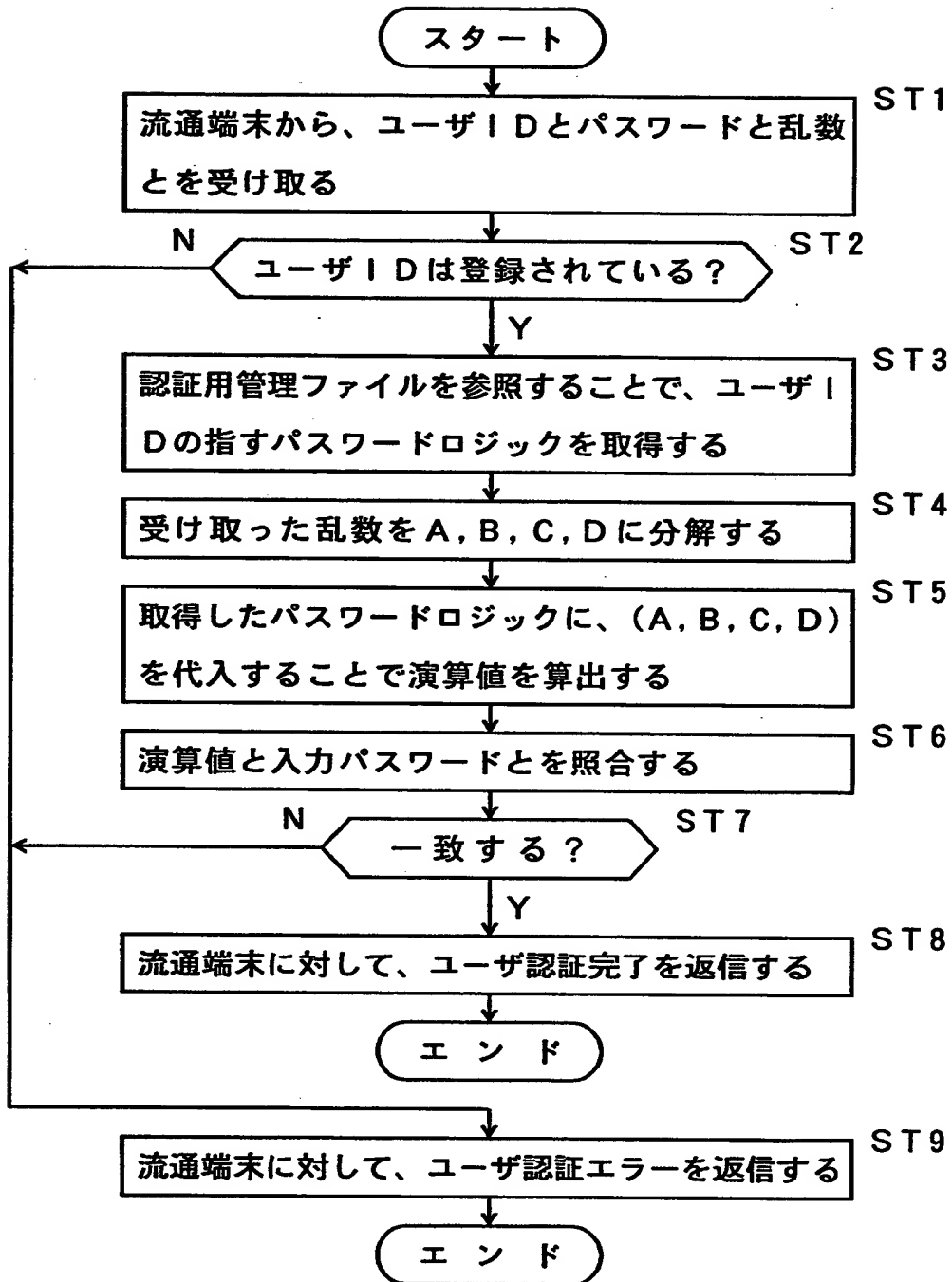
【図 17】

対 話 プ ロ グ ラ ム の 処 理 フ ロ ー



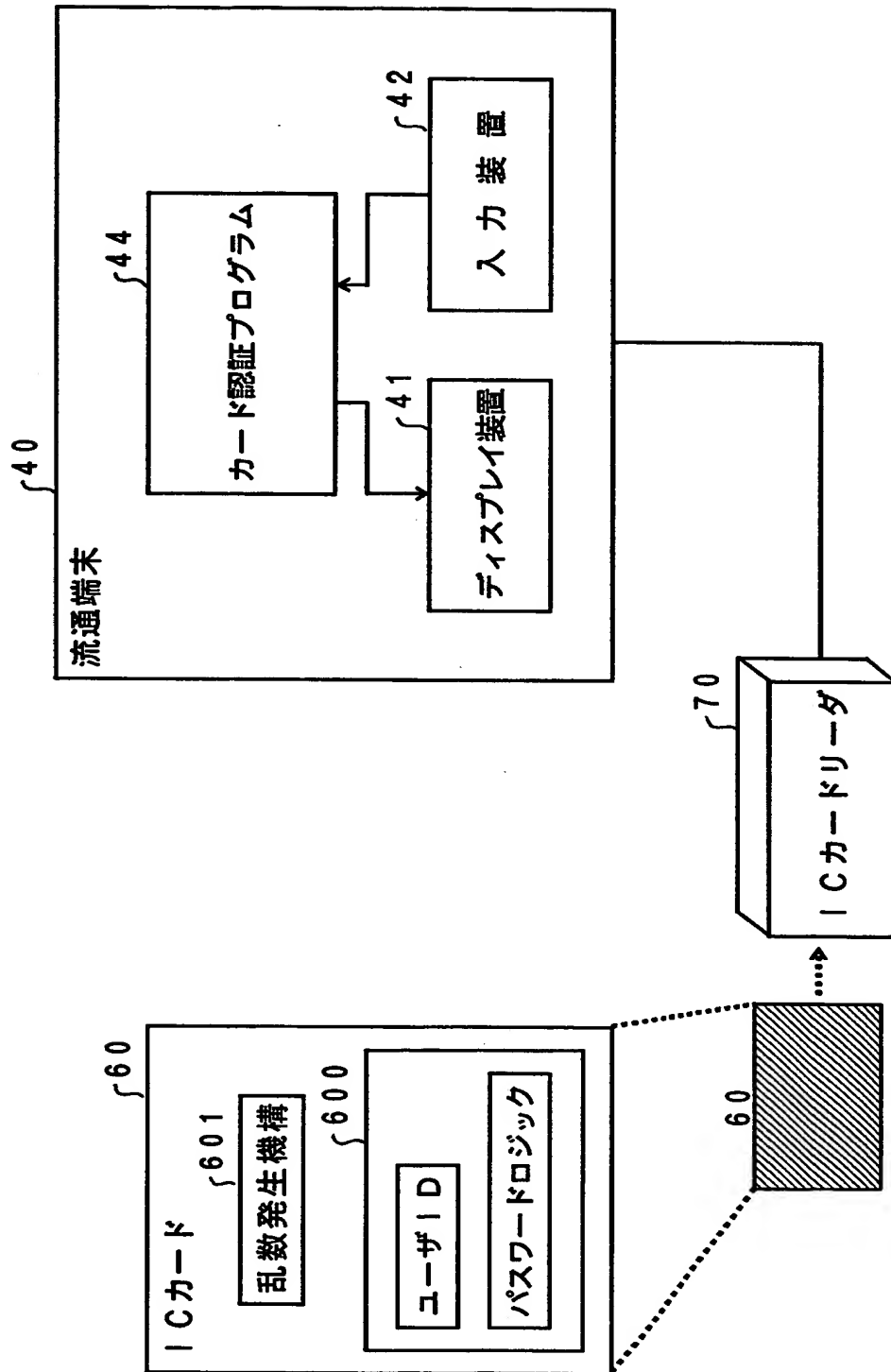
【図 18】

認証プログラムの処理フロー



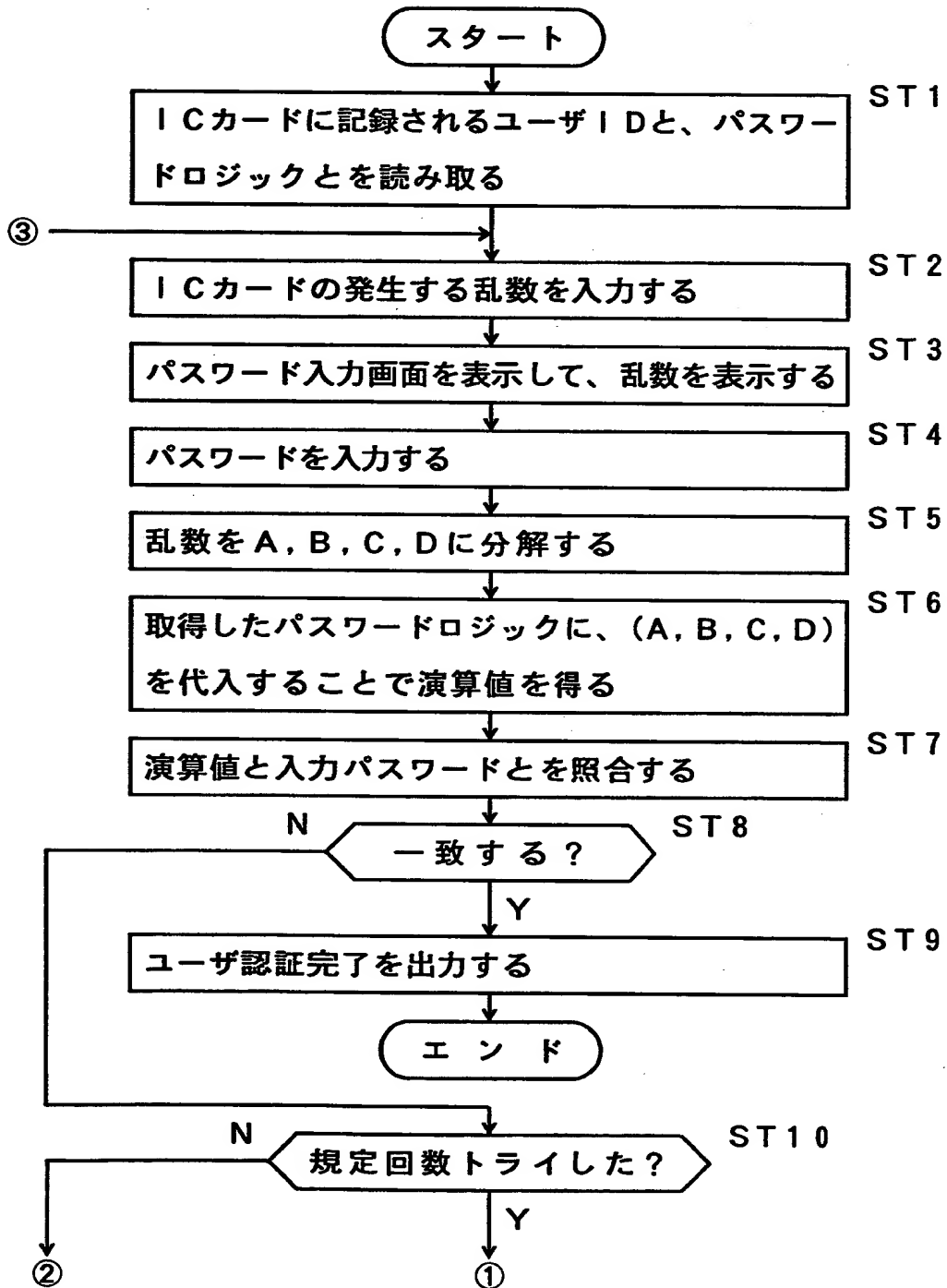
【図 19】

本 発 明 の 一 実 施 例



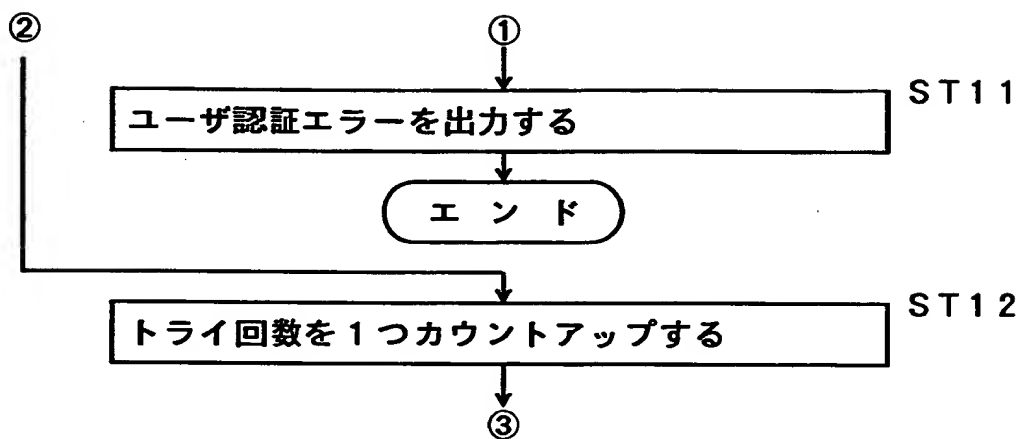
【図 20】

カード認証プログラムの処理フロー



【図 21】

カード認証プログラムの処理フロー



【書類名】 要約書

【要約】

【課題】 本発明は、ユーザ認証に用いるユーザ認証装置に関し、ユーザやシステムに負荷をかけることなく高いセキュリティを実現することを目的とする。

【解決手段】 ユーザに提示される乱数とユーザ認証対象に対応した計算式とから、ユーザ認証に用いる数値を算出する算出手段と、その乱数の提示に応答して入力されてくる数値と、算出手段の算出する数値とが一致するの否かを判断する判断手段とを備えるように構成する。この構成に従って、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。そして、ユーザは計算式のみを覚えれば足りるとともに、システムは計算式のみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社